

EventTracker Enterprise User Guide

Version 7.3

Copyright

All intellectual property rights in this work belong to Prism Microsystems, Inc. The information contained in this work must not be reproduced or distributed to others in any form or by any means, electronic or mechanical, for any purpose, without the prior permission of Prism Microsystems, Inc., or used except as expressly authorized in writing by Prism Microsystems, Inc.

Copyright © 1999 - 2012 Prism Microsystems, Inc. All Rights Reserved.

Trademarks

All company, brand and product names are referenced for identification purposes only and may be trademarks or registered trademarks that are the sole property of their respective owners.

Disclaimer

Prism Microsystems, Inc. reserves the right to make changes to this manual and the equipment described herein without notice. Prism Microsystems, Inc. has made all reasonable efforts to ensure that the information in this manual is accurate and complete. However, Prism Microsystems, Inc. shall not be liable for any technical or editorial errors or omissions made herein or for incidental, special, or consequential damage of whatsoever nature resulting from the furnishing of this manual, or operation and performance of equipment in connection with this manual.

Contents

About this Guide	xv
Purpose of this guide.....	xv
Who should read this guide	xv
Typographical Conventions	xv
Document Revision Control.....	xvi
How to Get In Touch.....	xvii
Documentation Support	xvii
Customer Support	xvii
Related Documents	xvii
Chapter 1 Getting Started	18
About EventTracker	19
EventTracker Services and Ports	20
Starting EventTracker	22
Event-O-Meter	30
Incorporating Your Company Logo	31
EventTracker Components.....	32
EventVault Manager.....	32
Events Knowledge Base	34
Replacing Outdated CRL	34
Updating EventTracker Users List	37
Exiting EventTracker	38
Chapter 2 Analyzing Incidents	42
Incidents Dashboard.....	43
To analyze incidents dashboard.....	43
Tuning alerts configuration.....	44
View alert flex report	45
Log search.....	46
Knowledge Base.....	48
'Search Incidents' window	48
Search Criteria	53
Web Slices	56
Adding Web Slices to the Favorites Bar.....	56
Chapter 3 StatusTracker	58
About Status Tracker	59
Creating User Defined Group.....	63
To add group	63
To add systems in the group.....	64
To add application(s) for monitoring.....	66
Edit Applications	72
View Request Status.....	75
Delete Group	76
Remove Monitoring	77
Add removed systems for monitoring.....	79
Change Status	80
Edit Resources.....	82
Polling Summary	84
Add Notes.....	85
StatusTracker Reports	86

Chapter 4 Analyzing Enterprise Activities	90
Monitoring Enterprise Activities.....	91
Enterprise Activity Dashlets.....	91
Adding Behavior Dashlets	92
Analyzing User Activities.....	94
Non-admin User Activities.....	94
Admin User Activities	94
Analyze User Activities in Behavior Dashboard.....	95
Analyzing Activities per System	101
Analyzing IP Addresses by Traffic	102
Analyzing Processes by Occurrence	106
Analyzing Events by Occurrences.....	109
Analyzing Log on Failure Activity	110
Analyzing RunAway Process Activity	111
Analyzing Software Activity	112
Analyzing Network Activity	113
Analyzing Application Activity	114
Analyzing USB Activity	114
Configuring Behavior Filters.....	116
Volume Analysis	119
Enterprise Activity Behavior Settings	122
Behavior Rules.....	123
Managing Behavior Rules	125
Adding Behavior Rules.....	126
Geo Location	131
Chapter 5 Dashboard	133
Keyword Indexed Dashboard	133
Keyword Indexed Dashboard	134
Viewing Security Dashboard	134
Configuring Category Dashlets.....	137
Customizing Security Dashboard	141
Resetting Personalization.....	143
Compliance Dashboard	143
Chapter 6 Reports	146
Alphabetical Reports.....	147
Security/Operations/Compliance and My EventTracker Reports	148
Security/Operations/Compliance Reports	148
Security	148
Operations	148
Compliance.....	149
My EventTracker Reports.....	150
Searching Security/Operations/Compliance/My EventTracker Reports	151
Enterprise Feeds.....	152
My Feeds	152
Reports Wizard	153
Reports Exceptions	154
Refine & Filter Options.....	155
Scheduling Reports.....	156
Defining / Scheduling Reports Using Existing Configuration.....	159
Viewing Scheduled Reports History and Details	159
Sending Published Reports via E-mail.....	160

Running Scheduled Reports On Demand.....	160
On Demand Reports	161
Generating On Demand Reports – Foreground.....	162
Generating On Demand Reports – Foreground – Power Viewer.....	163
Generating On Demand Reports – Foreground – Smart Viewer	164
Generating On Demand Reports – Background (Queued)	165
Defining Reports	166
Report Calendar	167
Report Status Snapshot.....	169
Favorites.....	170
Adding to Favorites	170
Viewing the Favorites list	170
Chapter 6 Analyzing Netflow Data	172
What is Netflow?	173
Terminology.....	173
EventTracker Netflow Analyzer	174
How it benefits you	174
Enabling EventTracker Netflow Receiver	174
Interpreting Netflow Data	176
Interface Manager	179
Chapter 7 Viewing Windows System Status	182
Viewing Managed Windows System Status	183
Loading Tabs Together.....	185
Chapter 8 Viewing Logs	187
Viewing Logs	188
Chapter 9 Configuring Manager	191
Configuration- Alert Events	192
Enabling Alert Notification Status Tracking	192
Purging Alert Events Cache.....	192
Enabling Remedial Actions	193
Suppressing Duplicate Alerts	193
Configuration- Correlation Receiver	194
Configuration- Keyword Indexer	194
Enabling Keyword Indexing.....	194
Configuration- EventTracker Knowledge Base Web Site.....	196
Configuration- Logon Banner.....	196
Configuration- Cost Savings.....	197
Syslog / Virtual Collection Point.....	197
Monitoring syslogs	197
Virtual Collection Points.....	198
Configuring EventTracker Receiver to Listen on Multiple Ports.....	199
Virtual Collection Points for syslogs	199
Configuring EventTracker Receiver Ports.....	199
Forwarding Raw syslog Messages	200
Virtual Collection Points for Windows Events	200
Example Scenario	200
Computer: Sys1 – Configuring Ports	201
Upgrading Agent (Sys2) from Manager (Sys1).....	201
Upgrading Agent (Sys3) from Manager (Sys1).....	202
Direct Log Archiver / Netflow Receiver.....	202
Configuring Direct Log File Archiver.....	202

Vulnerability Scanners	203
Qualys Parser	203
Nessus Parser	204
SAINT Parser	204
eEye Retina Parser	205
Rapid7 NeXpose Parser	206
Enabling NetFlow Receiver	207
Adding Netflow Receiver Port	207
Agent Settings	208
Configure Agent File Transfer Settings	208
Configuring Config Assessment Settings	209
Configuring E-mail Settings	209
Manage Email Accounts	210
Configuring StatusTracker Settings	213
Chapter 10 Configuring Alerts and Alert Notifications	214
Alerts	215
Risk Metrics	215
Add Custom Alerts	216
Add Pre-defined Categories as Alerts	224
Deleting Alerts	225
Configuring Alert Actions – Manager Side	225
Configure E-mail Alert Action	225
Configure Audible Alert Action	226
Configure Console Message Alert Action	227
Configure RSS Alert Notification	228
Forward Events as SNMP Traps	229
Forward events as syslog messages	230
Executing Remedial Action at EventTracker Manager Console System	232
Executing Remedial Action at EventTracker Windows Agent System	233
Edit Alert Actions	234
Fault Monitoring/Alerting/Acting	235
Remedial Actions	235
How it works	235
Remedial Actions Events & Traps	237
How Remedial Actions Help	237
Enable Remedial Action	237
Chapter 11 Configuring Event Filters	239
Filtering Events from View	240
Configuring Event Filters	240
Configure Event Filters with Exception	242
Understanding Filters and Filter Exceptions	242
Chapter 12 Configuring Reports Settings	244
Configuring Published Reports Settings	245
Configure Cost Saving Reports Settings	247
Chapter 13 Analyzing Logs	248
Reg-Ex Help	249
How to Create a New Group	249
About Parsing Rule	252
The Need for Adding Parsing Rule in Flex Report	252
How EventTracker Helps?	253
Prior Knowledge	253
Components of Parsing Rules	253

What is Token?	253
Parsing Rule Occurrences	254
What is Display Name?	254
What is Separator?	254
What is Terminator?	254
Token templates	258
Analyzing Logs.....	258
Flex Reports - Summary - On Demand	258
Standard Column Flex reports.....	258
Quick View (Smart Viewer)	266
Custom Column Flex Reports.....	266
Flex Reports - Detail - On Demand	268
Standard Column Flex Reports.....	268
Quick View.....	272
Custom Column Flex Reports.....	273
Flex Reports - Trend - On Demand.....	277
Standard Column Flex Reports.....	277
Flex Reports - Summary - Queued	280
Standard Column Flex Reports.....	280
Custom Column Flex Reports.....	281
Flex Reports - Detail - Queued.....	283
Standard Column Flex Reports.....	283
Custom Column Flex Reports.....	284
Flex Reports - Trend - Queued	287
Standard Column Flex Reports.....	287
Flex Reports - Summary - Scheduled	291
Standard Column Flex reports.....	291
Custom Column flex reports	292
Flex Reports - Detail - Scheduled	293
Standard Column Flex reports.....	293
Custom Column Flex reports.....	294
Flex reports - Trend - Scheduled	296
Flex reports - Summary - Defined.....	297
Standard Column Flex reports.....	297
Custom Column Flex reports.....	298
Flex Reports - Detail - Defined.....	299
Standard Column Flex reports.....	299
Flex reports - Trend - Defined	300
Searching generated Queued Flex Reports.....	301
Exporting Summary Report on Generated Flex Reports	301
Flex - Report Queue Statistics	302
Flex Reports Queue Statistics - Admin.....	302
Analyzing Alerts	302
Alert Flex reports - On Demand	302
Quick View.....	303
Alert Flex reports - Queued.....	303
Alert Flex reports - Scheduled.....	305
Analyzing Log Volume.....	306
Flex Reports Logs - On Demand	306
Flex reports Logs- Queued.....	308
Flex reports Logs- Scheduled.....	310
Analyzing Suspicious Traffic.....	311
Flex reports Suspicious Traffic - On Demand.....	311
Flex Reports Suspicious Traffic - Queued	312

Flex Reports Suspicious Traffic - Scheduled	313
Analyzing ROI	314
Person Hour	314
Chapter 14 Configuring RSS Feeds	317
RSS Feeds	318
Adding RSS Feeds.....	318
Delete RSS Feeds.....	320
Chapter 15 Managing System Groups	321
About Systems Manager.....	322
Discover Modes	323
Auto Discover Mode.....	323
Manual Mode	324
Manually Adding Computers	324
Adding a Single Computer.....	324
Adding a Group of Computers	326
Adding a Group of Computers from an IP subnet.....	327
Logical System Groups.....	328
Creating a New Logical Group – System Type	328
Creating a New Logical Group – IP Subnet.....	329
Creating a New Logical Group – Manual Selection	330
Modifying a Group	332
Deleting a Group.....	333
Viewing System Details	334
Restarting Agent Service.....	335
Querying Agent Service Status	337
Querying Agent Version	338
Managing Asset Value	339
Deleting Systems	341
Searching Systems	342
Setting Sort by Option.....	342
Chapter 16 Managing Windows Agents	344
Agent for Windows Systems	345
Pros	345
Cons.....	346
Deploying Agents	346
Pre-installation Procedures	346
Installing EventTracker Windows & Change Audit Agents	346
View System Status.....	352
Uninstalling EventTracker Windows & Change Audit Agents	354
Upgrading EventTracker Windows & Change Audit Agents.....	356
Removing Windows Agent Components	357
Vista Agent	358
Event Publishers in Windows Event Log	358
Event Logs and Channels in Windows Event Log.....	358
Event Consumers in Windows Event Log	359
Prerequisites.....	359
Installing / Uninstalling Vista Agent	359
Filtering Events	359
Monitoring EVTX Logfiles.....	360
Configuring Windows Agent.....	361
Basic Configuration	361
Forwarding Events to Multiple Destinations	362
Event Delivery Modes	366

Modifying Event Delivery Modes	367
Modifying Event Delivery Modes for Syslog	368
Removing Managers	369
Saving Agent configuration	369
Filtering Events	373
Filtering Events with Exception	375
Filtering Events with Advanced Filters	377
Enabling High Performance Mode	380
Enabling SID Translation	380
Monitoring System Health	381
Adding USB Device in the Exception List	383
Monitoring Applications	384
Filtering Applications that need not be monitored	385
Filtering Applications that need to be monitored	386
Monitoring Services	386
Configuring Service Restart List	387
Filtering Services	388
Monitoring Logfiles	388
Viewing File Details	396
Deleting Log File Monitoring Settings	396
Searching Strings	397
Viewing File Details – Web UI	399
Viewing Search Strings – Web UI	400
Monitoring Check Point Logs	401
Monitoring VMware Logs	403
Monitoring Network Connections	405
Excluding Network Connections	407
Including Network Connections for Monitoring	412
Suspicious Connections	414
Monitoring Suspicious Connections	415
Adding Programs to the Trusted List	418
Adding Firewall Exceptions to the Trusted List	419
Monitoring Processes	420
Removing Processes from ‘List of Filtered Processes’	421
Maintaining Log Backup	421
Transferring Log Files	423
Assessing Configuration	426
Applying Configuration Settings to Specified Agents	426
Backing up Current Configuration	428
Protecting Agent Configuration Settings	429
Syslog FTP Sever	430
Enabling Remedial Action	438
Generating System Report	438
Viewing Reports	439
Managed System Report	440
Unmanaged System Report	440
All System Report	441
Chapter 17 Agentless Monitoring of Windows Systems	442
Agentless Monitoring	443
Pros	443
Cons	443
Adding Systems for Agentless Monitoring	443
Chapter 18 EventVault Manager	449

About EventVault.....	450
EventTracker Scheduler Service	450
EventTracker Scheduler service – Collection Master Console	450
EventTracker Scheduler service – Collection Point Console	450
Viewing CAB Files	451
Configuring EventVault	451
Verifying EventBox Integrity.....	452
Viewing CAB Files by Port Number.....	453
Chapter 19 Managing Category Groups and Categories	455
Managing Category Groups	456
Creating Category Groups	456
Modifying Category Groups.....	457
Deleting Category Groups	457
Managing Categories	457
Creating Categories	458
Modifying Categories.....	459
Deleting Categories	460
Deleting Event Rules	460
Adding Categories as Alerts	461
Chapter 20 EventTracker Utilities.....	462
EventTracker Desktop Control Panel.....	463
EventVault Warehouse Managers.....	464
Saving EventBox Metadata	465
Backing up EventVault Data.....	466
Extracting EventBox Data	466
Moving CAB files.....	467
Deleting an EventBox	467
Viewing CAB Files by Port Number.....	468
EventTracker Diagnostic Tool.....	469
Setting Debug Levels	472
Obfuscating Classified Information	475
Diagnostic Alert	478
Export and Import Utility.....	480
Exporting Categories.....	480
Exporting Filters.....	481
Exporting Alerts.....	482
Exporting System Groups	483
Exporting Scheduled Reports.....	484
Exporting RSS Feeds.....	484
Exporting Behavior Rules.....	485
Importing Categories	486
Importing Filters.....	487
Importing Alerts	487
Importing System Groups	488
Importing Scheduled Reports.....	490
Importing RSS Feeds	491
Importing Behavior Rules	491
Importing SCAP Content	492
Appending CAB Files	493
Event Traffic Analysis	499
Traffic Analysis – View by Category.....	500
Correlating Events	501
Traffic Analysis – View by Event Id	502

Traffic Analysis – View by Custom Selection.....	503
Traffic Analysis – Keyword Analysis	504
Adding Keywords for Analysis.....	506
Adding Commonly Occurring Words to Exclude from Analysis	507
Windows Agent Management Tool	509
Accessing Agent Management Tool	509
Querying Agent Service Status - System	509
Querying Agent Service Status - Group	511
Querying Agent Service Status - All.....	512
Querying Agent Service Status – Custom	512
Restarting Agent Service - System.....	513
Restarting Agent Service - Group	513
Restarting Agent Service - All	513
Restarting Agent Service - Custom	514
Querying Version of the Agent Service - System.....	515
Querying Version of the Agent Service - Group.....	515
Querying Version of the Agent Service - All	515
Querying Version of the Agent Service - Custom	516
Removing the Agent Component	517
Deleting Systems from the agent service	517
SCAP Benchmark Profile Editor	517
EventTracker Event Correlator	521
What is Event Correlation	521
Event Correlation Engine	522
How Event Correlator works	522
Configuration User Interface	522
Viewing Published Legacy Reports.....	524
License Manager.....	524
EventVault Explorer	530
Performing search in EventVault Explorer.....	530
Configuring EventVault Explorer to use remote Sqlserver.....	536
Chapter 21 Managing Users.....	540
EventTracker Roles, Permissions & Privileges	541
Roles.....	541
Privileges.....	541
Permissions	541
Promoting a Non-Admin User as an Administrator.....	544
Demoting an Administrator	546
Assigning Permissions to Non-Admin Users	547
Viewing Permissions	548
Assigning Privileges to Non-Admin Users.....	548
Viewing Privileges	550
Verification	551
Chapter 22 Collection Point Model	554
What is Collection Point model	555
Scalability	555
Real world scenarios.....	555
Chapter 23 Collection Master	559
Starting Collection Master.....	560
Viewing Collection Point Details.....	561
Configuring Collection Master listening port	562
Deleting CAB Files.....	562

Deleting Collection Point Details	563
Chapter 24 Collection Point.....	564
Viewing Collection Point Configuration	565
Adding Collection Masters	566
Editing Collection Master Settings	567
Deleting Collection Master Settings	567
Viewing CAB Status	567
Resending CAB Files	568
Chapter 25 Auditing Changes.....	569
Why Should I Audit Changes?.....	570
Change Audit Dashboard	570
Viewing Last changes	572
Setting Dashboard Preferences	574
Viewing Change Details.....	577
Authorizing Unauthorized Changes.....	578
Viewing Access History.....	581
Viewing Additional Info on Files	583
Enabling O/S Auditing on Folder(s)	583
Enabling O/S Auditing on Registry Keys.....	589
Assessing the Changes	591
Analyzing Policy Comparison Results.....	593
Scheduling Change Assessment	594
Editing Change Assessment Schedules.....	596
Running Schedules On Demand	596
Deleting Scheduled policies.....	597
Viewing Policy Dashboard	597
Customizing the Policies Dashboard	598
EventTracker Inventory Manager	601
Chapter 26 Assessing Configuration Using SCAP	607
NIST Guidelines	608
How EventTracker Helps?	608
How does it work?.....	608
NIST Benchmarks Implemented in EventTracker	609
What is FDCC?.....	612
What is SCAP?.....	613
What is SCAP content?.....	614
How SCAP is Implemented in EventTracker.....	614
What is CVE?.....	615
How CVE Standard is Implemented in EventTracker	615
What is CCE?	615
How CCE Standard is Implemented in EventTracker	616
What is CPE?.....	616
How CPE Standard is Implemented in EventTracker	616
What is XCCDF?.....	616
How XCCDF Standard is Implemented in EventTracker.....	617
What is OVAL?	617
How OVAL Standard is Implemented in EventTracker.....	618
What is CVSS?.....	618
How EventTracker supports CVSS	618
FDCC and SCAP	618
FDCC Reporting Format	619

Assessing Managed Computers	620
Viewing Assessment Results	621
Viewing Assessment Details	624
Exporting Assessment Details	627
Searching Rules by CCE Id	628
Adding Deviation	629
Publishing FDCC Report	632
Viewing OVAL Result File	633
Creating FDCC Report Bundle	634
Scheduling Config Assessment	636
Viewing Schedule Details and History	638
Editing Config Assessment Schedules	639
Searching Published Reports	640
Exporting Summary on Published Reports	641
Importing SCAP Benchmarks	641
How To	645
How to View Failed Config Assessment Results?	645
How to View OVAL Definitions?	646
How to View CCE Id of a Rule?	648
How to Locate a Rule Using CCE Id Search?	648
How to View Status and Publication Date of a Benchmark?	649
How to View Patch Results and CVE IDs?	650
How to Verify XCCDF Content is not Applicable to a Platform?	653
How to Locate the Config Assessment Result Folder on Server?	654
Config Assessment Dashboard	655
Chapter 27 Tag Cloud Weighting	660
Tag Clouds	661
Assigning Weights to Tags	662
Assigning Weights to Multiple Tags	664
Adding Keywords as Tags	664
Chapter 28 Searching Logs	665
Searching Logs	666
How Indexing Works in Tandem with Log Search?	666
Key Features	666
Pros	667
Cons	667
Benchmark Report on Keyword Indexer	667
Keyword Indexer Overview	668
Basic Search	668
Advanced Search	669
Chapter 29 Securing EventTracker	670
Server Hardening	671
Encryption	671
Enabling Encryption from the Agent	672
Enabling Encryption from CP to CM	672
Using https to Reach the EventTracker Console	672
Chapter 30 Add-in Software Modules	673
TrapTracker	674
StatusTracker	674
Solaris Agent	675
Benefits of Solaris Agent	675
Purchase	675

Appendix – HIPAA	676
HIPAA Compliance Reports	676
User Logon report.....	676
User Logoff report	676
Logon Failure report	676
Audit Logs access report.....	676
Appendix – SOX.....	677
Sarbanes – Oxley Compliance Reports	677
User Logoff report	677
User Logon report.....	677
Logon Failure report	677
Audit Logs access report.....	677
Security Log Archiving Utility	677
Track Account management changes.....	678
Track Audit policy changes.....	678
Track individual user actions.....	678
Track application access	678
Track directory / file access	678
Appendix – GLBA.....	679
GLBA Compliance Reports.....	679
User Logon report.....	679
User Logoff report	679
Logon Failure report	679
Audit Logs access report.....	679
Appendix – Security Reports	680
Security Reports	680
Successful and failed file access	680
Successful logons preceded by failed logons	680
Audit log cleared events by user	680
Invalid logons by date	680
Daily reboot statistics	680
CPU load peaks by computers.....	680
Account usage outside of normal hours	680
Audit policy history	681
Accounts that were never logged on	681
Administrative Access to Computers	681
File Access by User	682
Hot fixes by Computer	682
Last logon by Domain Controller	682
User Account Locked Out.....	683
Appendix – BASEL II	684
BASEL II	684
Appendix – FISMA.....	685
FISMA	685
FISMA Sec. 3505.....	685
FISMA Sec. 3544	685
Appendix – PCI DSS.....	686
PCI DSS	686
Glossary	687
Index.....	691

About this Guide

Purpose of this guide

This guide will enable you to use every option of EventTracker and provides detailed procedures for the same.

Who should read this guide


Intended audience:

- Administrators who are assigned the task to monitor and manage events using EventTracker
- Operations personnel who manage day-to-day operations using EventTracker

Typographical Conventions

Before you start, it is important to understand the typographical conventions followed in this guide:

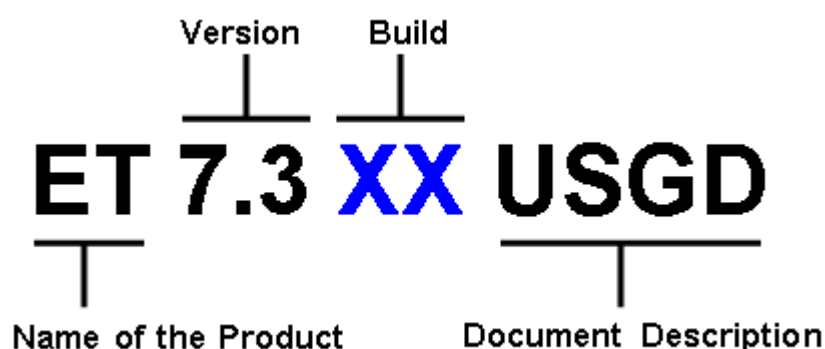
Table 1

This	Represents
Italics	References to other guides and documents.
Bold	Input fields, radio button names, checkboxes, drop-down lists, menus, and menu options, buttons on the screen and keyboard keys.
{Text_to_customize}	A placeholder for something that you must customize. For example,{Server_Name}would be replaced with the name of your server/ machine name or an IP address.
Constant width	Text that you enter, program code, files and directory names, function names.
	A Note, providing additional information about a certain topic.
Sidebar information	Important additional information about topic on the page.

Document Revision Control

This section defines the conventions followed for the document revision control number. The revision control number is an alphanumeric identifier, unique to the document. The components of the acronym identify the following:

- First two letters – name of the product
- Second two numbers – version of the product
- Third two numbers – build of the product
- Last four letters – document description



The document revision control number for this guide is as given below:

Table 2

File Name	EventTracker v7.3 Enterprise User Guide
Description	Updated in accordance with release version 7.3 build XX.
Status	Draft
Release Date	July 27, 2012

How to Get In Touch

The following sections provide information on how to obtain support for the documentation and the software.

Documentation Support

Prism Microsystems, Inc. welcomes your comments and suggestions on the quality and usefulness of this document. For any questions, comments, or suggestions on the documentation, you can contact us by e-mail at support@eventtracker.com

Customer Support

If you have any problems, questions, comments, or suggestions regarding EventTracker, contact us by e-mail at support@eventtracker.com While contacting customer support, have the following information ready:

- Your name, e-mail address, phone number, and fax number
 - The type of hardware, including the server configuration and network hardware if available
 - The version of EventTracker and the operating system
 - The exact message that appeared when the problem occurred or any other error messages that appeared on your screen
 - A description of how you tried to solve the problem
-

Related Documents

[Install Guide](#)

[Upgrade Guide](#)

[Direct Log Archiver](#)

[Agent DLA](#)

[Virtual Collection Points](#)

[Log Search](#)

[Parsing Rule](#)

[Change Audit](#)

[Installing & Customizing Web Server \(IIS\)](#)

[IIS Custom Error Setting](#)

[Securing IIS Web Server with SSL](#)

Chapter 1

Getting Started

In this chapter, you will learn about:

- [EventTracker Services and Ports](#)
- [EventTracker Components](#)

About EventTracker

EventTracker framework is Prism Microsystems, Inc's flagship event log monitoring and management product. EventTracker is a reliable and practical software-only solution, to monitor, track, and manage critical events that occur in Windows 2000/2003/XP/Vista/2008/2008R2/MSCS systems and UNIX-style Syslog in your enterprise. Installation of EventTracker is quick, simple, and intuitive. EventTracker comes with a thorough resource kit with several nifty utilities, which alleviates the pain of day-to-day administration of your enterprise network. Log Volume Analysis is similar to Log Analysis but with more bells and whistles, which gives you an incisive insight into the event traffic flow in your enterprise.

- Agent Optional Architecture
 - Cross-platform support
 - Centralized Warehouse
 - Auto back-up / clear native event logs
 - Real-time Alerts
 - Event Correlation
 - User tracking
 - Process, network and service monitoring
 - Granular filtering
 - Change auditing
 - Configuration assessment
 - NetFlow monitoring
 - Virtual Collection Points
 - Execute Remedial Actions
 - Monitor file transactions that occur in the inserted media (USB or other devices)
 - Generate audit reports based on Collection Point Sites
 - Manage Active Directory (AD) Organizational Units (OU)
 - SID translation
 - Generate audit-ready compliance reports (HIPAA, SOX, FISMA, GLBA, PCI)
-

EventTracker Services and Ports

Table 3

Service	Description	Startup Type	Log on as	Allow service to interact with desktop
Event Correlator	Correlates the received events from the agent and performs the action based on the rules.	Automatic	Local System account	Yes
EventTracker Agent	Relays local log data and is usually managed by the central EventTracker Console. If uninstalled locally, corresponding changes will be necessary at the Console. May be restarted to pick up new configuration. Performs configuration assessment for received requests and sends back the assessment results.	Automatic	Local System account	Yes
EventTracker Alserter	Used by EventTracker to manage RSS notifications generated via Alerts.	Automatic	Local System account	Yes
EventTracker EventVault	An EventTracker component to compress and securely store the raw log data.	Automatic	Local System account	Yes
EventTracker Indexer	Responsible for indexing the key words of event properties. Event properties include Computer, Source, EventID, Domain, User, LogType, EventType, and Description.	Automatic	Local System account	Yes
EventTracker Receiver	Enables EventTracker to receive log data from the configured sources. If stopped, EventTracker cannot function. May be restarted to pick up new configuration.	Automatic	Local System account	Yes

Service	Description	Startup Type	Log on as	Allow service to interact with desktop
EventTracker Remoting	This service is used to send any request (like install agent/upgrade agent/uninstall agent etc.) to communicate with the EventTracker agent service.	Automatic	Local System account	Yes
EventTracker Reporter	Responsible for reports / Flex Report execution and log search.	Automatic	Local System account	Yes
EventTracker Scheduler	Used by EventTracker to initiate scheduled activities like CAB integrity verification, traffic analysis. Also initiates User Activity monitoring and 'Collection Point' related activities. Fetches configuration assessment requests from queue and dispatches the request to EventTracker agents running on target system.	Automatic	Local System account	Yes
WcwService	Used to take periodic snapshots and entertain change assessment requests.	Automatic	Local System account	Yes
Status Tracker	This service is used to keep track of system up and down.	Automatic	Local System account	Yes
Trap Tracker Receiver	Receives traps in the form of an alert or other asynchronous event about a managed subsystem.	Automatic	Local System account	Yes

NOTE

In case any EventTracker services are not running a warning message is displayed when you log in.

Figure 1

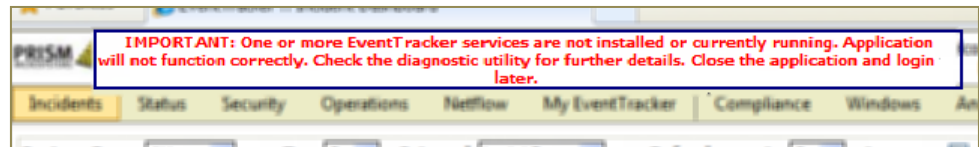


Figure 2

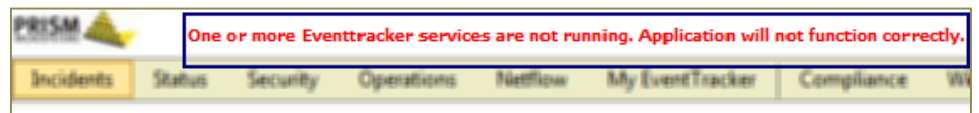


Table 4

EventTracker Module	Port(s)
EventTracker Agent	14506/TCP
Windows Receiver	14505(TCP/UDP) - optional and multiple VCP's can be configured
Syslog Receiver	514(UDP/TCP) can be configured to any number of ports
Collection Master	14507/TCP - optional and can be configured to any TCP port
Correlation Receiver	14509/TCP
EventTracker - Change Audit Agent	14502 (TCP bi-directional) - to transfer snapshot between client and Server. 14508 (TCP bi-directional) - used for real-time comparison of any system with the golden snapshot located at the server.
License Server	14503/TCP

Starting EventTracker

This option helps you start EventTracker.

To start EventTracker

- 1 Click **Start > Programs > Prism Microsystems > EventTracker > click EventTracker Enterprise.**

(OR)

Double-click the **EventTracker Enterprise** shortcut on your desktop.

EventTracker displays the login page.

Figure 3
EventTracker Login

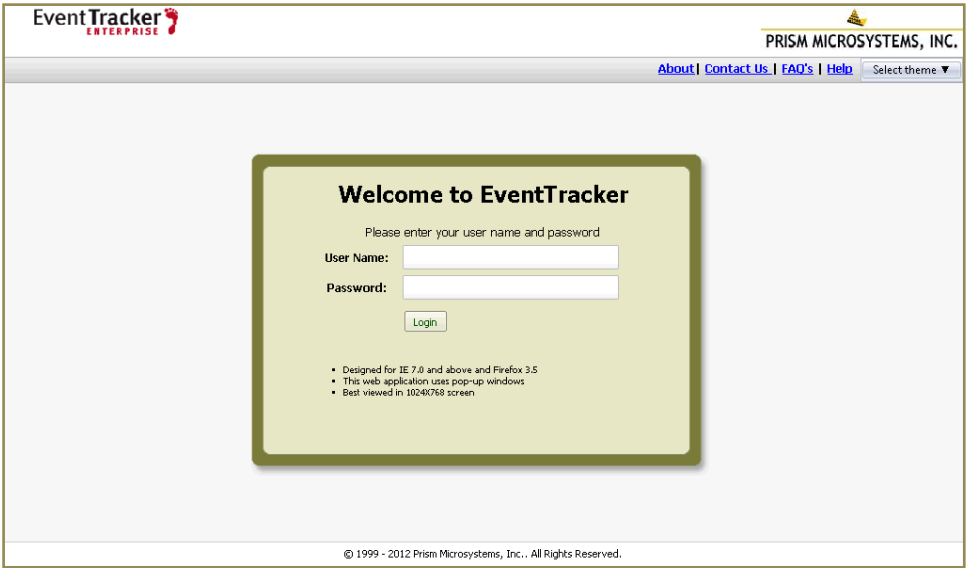
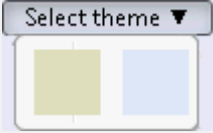


Table 5

Click	To
About	View license details and available features.
Contact Us	Go to 'Contact page' on Prism Web site.
FAQ's	Go to FAQ page.
Help	View online help.
Select theme	Apply themes to the web pages. The colour options available are gold and olive. 

EventTracker displays the logs processed information only when a CAB file is created locally on the server.

Figure 4
EventTracker Login



Welcome to EventTracker

Please enter your user name and password

User Name:

Password:

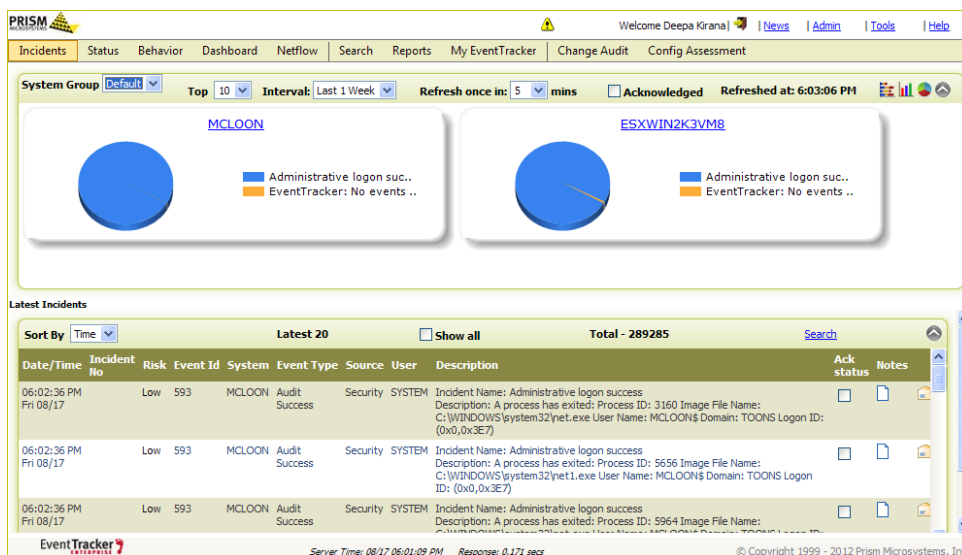
71,492 logs processed since install on Apr 16, 2012.
71,492 logs processed today.

- Designed for IE 7.0 and above and Firefox 3.5
- This web application uses pop-up windows
- Best viewed in 1024X768 screen

- 2 Type valid user credentials, and then click **Login**.

EventTracker displays the **Incidents** dashboard.

Figure 5
Incidents dashboard



- 3 Click the **Admin** dropdown at the upper-right corner.

EventTracker displays the **EventTracker Diagnostics** tab.

Figure 6
EventTracker
Diagnostics

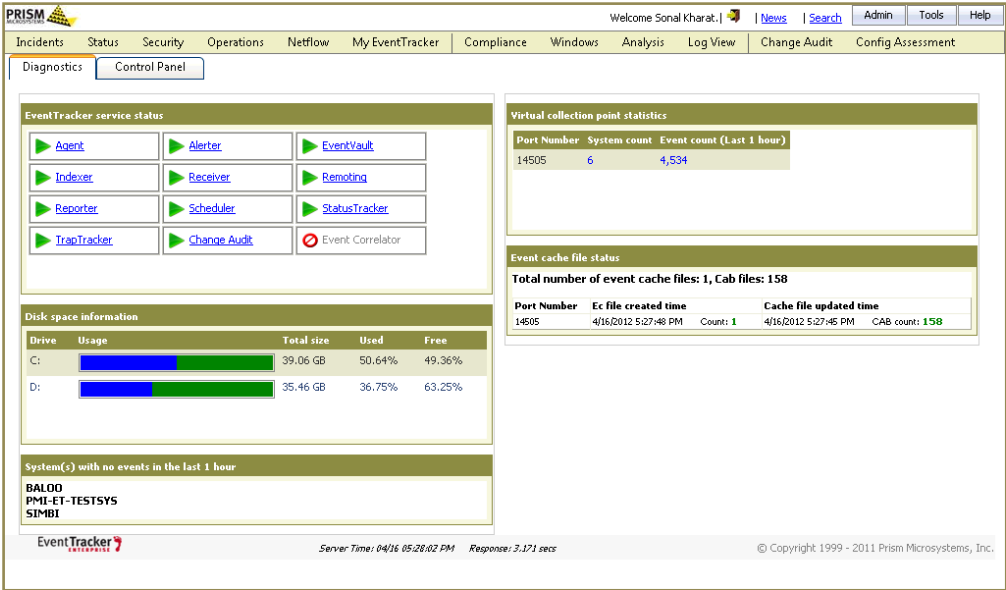
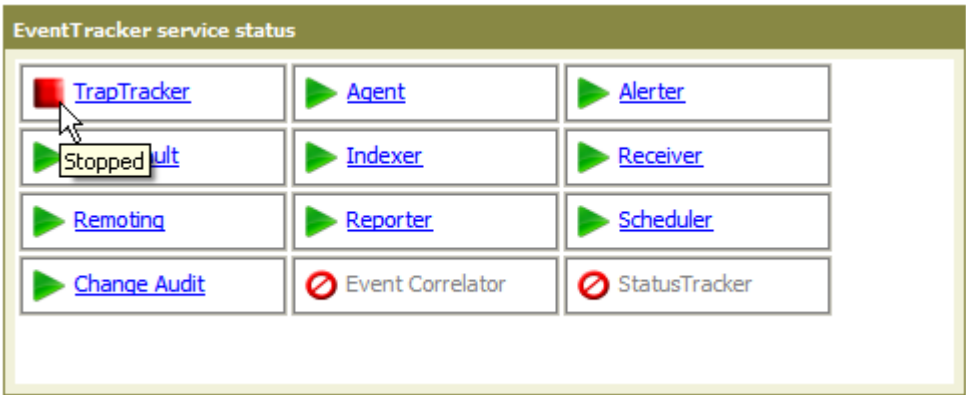


Table 6

Icon	Represents
EventTracker service status	
	Service stopped.
	Service is running.
	Service not installed

Move the mouse pointer over the service, EventTracker displays the status in a tooltip.

Figure 7
List of EventTracker
services and their
current status



- 4 Click the name of the service, EventTracker displays the description of the service in a pop-up window. (Example: Agent).

Figure 8
Service running
status

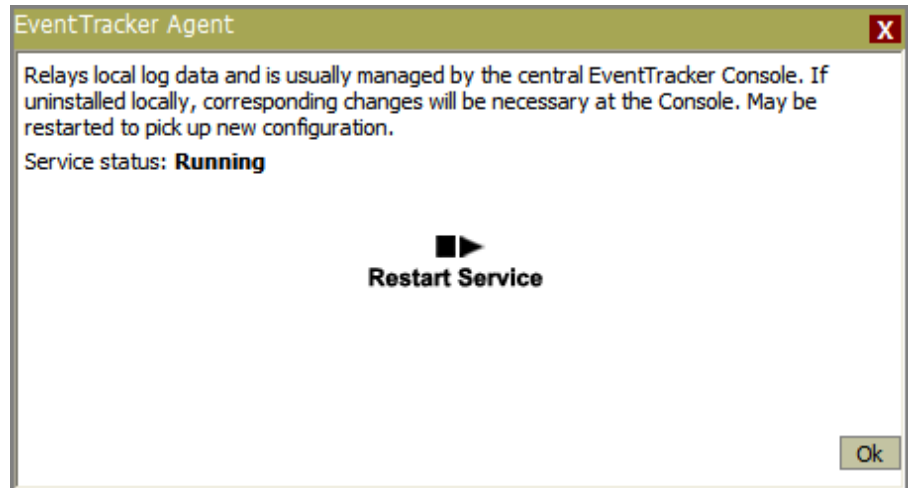
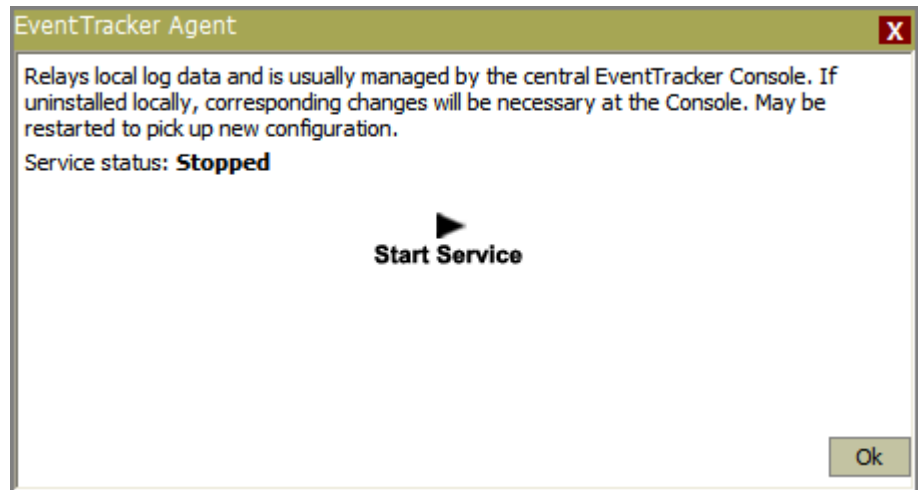


Figure 9
Service stopped
status





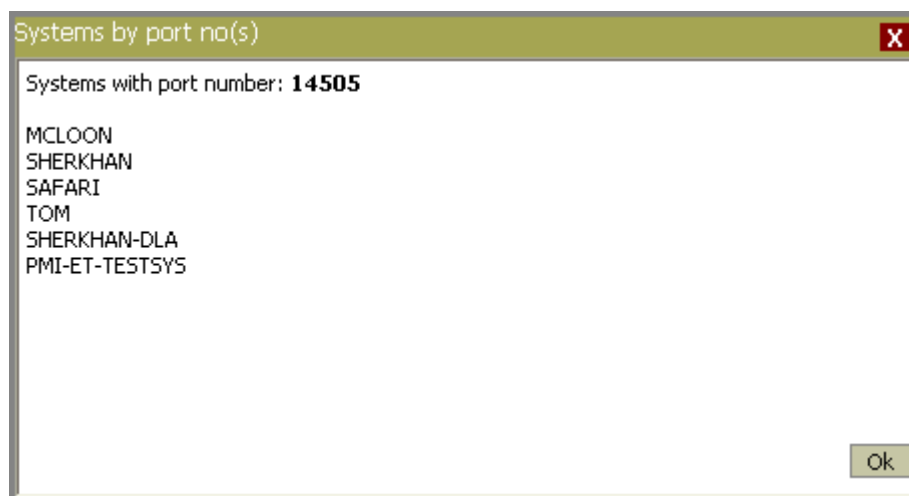
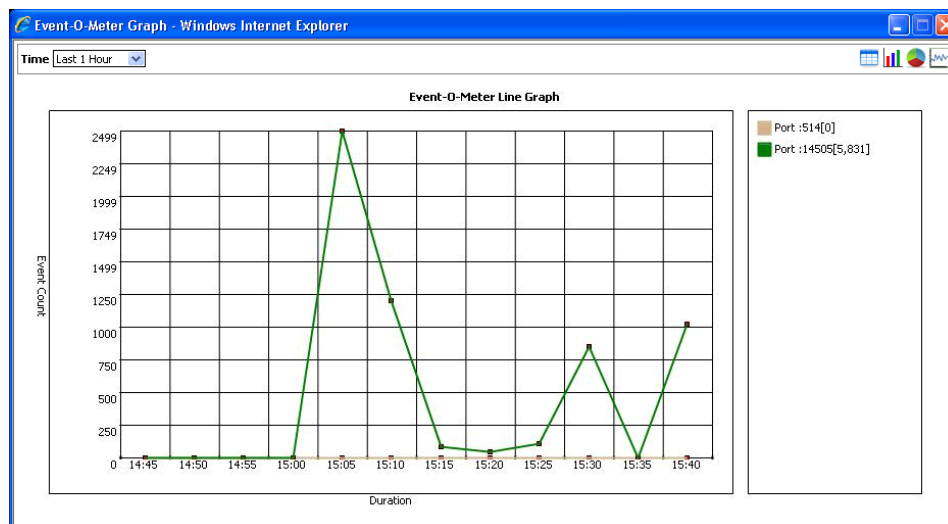
- 5 Click  icon to restart the service or click  icon to start the stopped service.
- 6 On the **Virtual collection point statistics** pane, click a hyperlink in the **System count** column to view the name of the systems forwarding events through a particular port.
EventTracker displays the name of the systems in a pop-up window.

Figure 10
Systems by port



- 7 Click a hyperlink in the **Event count** column to view the Event-O-Meter.

Figure 11
Event-O-Meter
graph


















- 8 On the **Disk space information** pane, move the mouse pointer over the graph, EventTracker displays the space used and free space information in a tooltip.
- 9 **System(s) with no events in the last 1 hour** pane will name the agent/ managed systems that have not reported to manager system in the last one hour.
- 10 **Event cache file status** represents the number of event cache files created and the number of cab files present on the machine.

- 11 Click the **Control Panel** tab.
 EventTracker displays the 'Control Panel' tab.

EventTracker Enterprise Control Panel tab consists of shortcuts that help you to quickly access EventTracker modules.





Figure 12
 EventTracker -
 Control Panel

Control Panel

 Alerts	Manage Alert configuration including notification and threat level.
 Behavior Rules	Define and manage behavior rules. These are used to display behavior dashlets in the Security, Operations tabs.
 Behavior Settings	Configuring settings for the Behavior module.
 Category	Event categories are used in reports, search, analysis and views. Pre-defined categories of knowledge are available. Users may create/edit categories.
 Event Filters	Configuring filters to avoid archiving specific events.
 Eventvault	Event log data is archived in the Eventvault. Manage archives and configure retention and validation.
 IP lookup configuration	IP lookup configuration.
 Manager	Manage EventTracker Console configuration; define Virtual Collection Points, enable syslog and netflow receivers etc.
 Parsing rules	Parsing rules.
 Report Settings	Manage settings that affect report generation and email delivery.
 RSS	Setup and manage RSS feeds.
 Systems	Manage the installation of EventTracker and Change Audit agents in the network.
 Users	Manage users defined in the EventTracker user group, their privileges and permissions.
 Weights	Assign weight values to Event Source, Event ID, Categories etc. These are used in the tag cloud display in the Search/Refine dialog.
 Windows Agent Config	Managing configuration of the windows agents.

To open a module, click the respective hyperlinks.

Table 7

Click	To
 Alerts	Manage alerts, alert actions, and alert threat level.
 Behavior Rules	Define and manage behavior rules. These rules could be added as behavior dashlets in the Security, Operations and My EventTracker tabs.
 Behavior Settings	Configuring settings for the 'Enterprise Activity Behavior' module.
 Category	Event categories are knowledge packs. You can add / modify / delete your own categories. You can also edit / delete pre-defined categories.

 Collection Master	EventTracker 'Collection Master' collects CAB files forwarded by Collection Point(s).
 Collection Point	Forwards CAB files to 'Collection Master(s)'.
 Event Filters	Configure manager side event filters.
 Eventvault	Functions as warehouse for CAB files. Manage archives and configure retention & validation.
 Manager	Define Virtual Collection Points, enable Syslog, configure DLA, enable NetFlow receivers etc.
 Report Settings	Manage settings that affect report generation and e-mail delivery.
 RSS	Configure and manage RSS feeds.
 Systems	Manage EventTracker Windows agent and Change Audit agent.
 Users	Manage privileges and permissions of the users defined in the EventTracker user group.
 Weights	Assign weight values to Event Source, Event ID, Categories, etc. These are used in the tag cloud display in the Search/Refine dialog (EventTracker Log Search).
 Windows Agent Config	Configure EventTracker Windows Agent.
 IP lookup configuration	Customizable IP Address verification/detailed information.

Table 8

TOOLS	
Event-O-Meter	View per port trends of events against specified time range.
EventVault Explorer	Run ad-hoc searches and save the data in a database. You can also configure EventVault Explorer to use remote Sqlserver database.
Favorites	Add bookmarks to often generated 'On Demand' Reports.
Log View	View per category per system logs. You have the liberty to choose category / system groups / systems.
Legacy Reports	View published legacy reports had you upgraded from earlier versions. NOTE: This option comes only if the existing version is upgraded from version 6.4.
Report Calendar	View time slots occupied by scheduled reports & analyses.(same change(s))

Report Status	Overview and Queue status of the On Demand / Queued reports and analyses. (replaces analyses with Flex)
Sitemap	View index of the web site.
Windows	View different activities that take place on a particular system. (Example: Software Installed, printer activity etc.)
Knowledge Base	Go to EventTracker Knowledge Base Web site http://kb.prismmicrosys.com/

Table 9:
Main menus

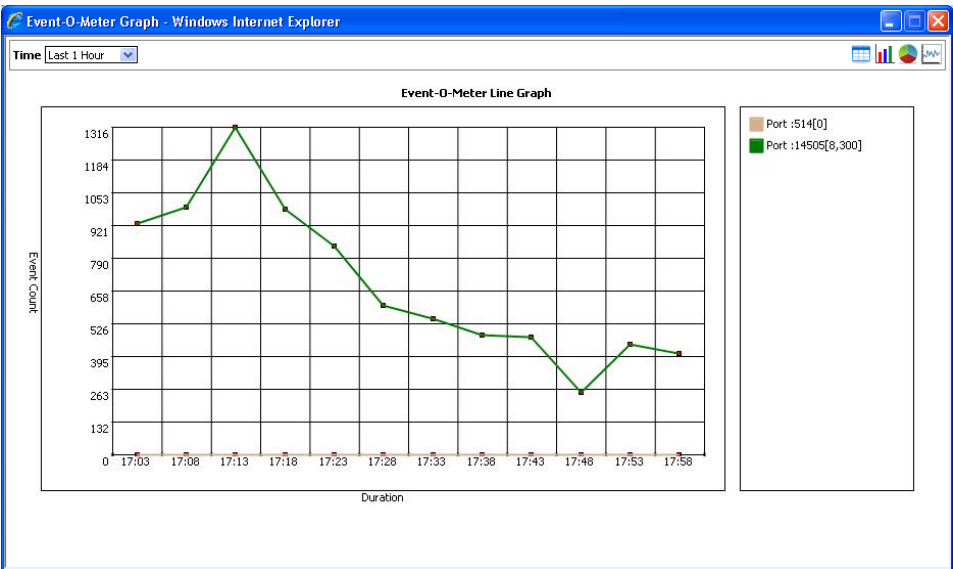
Click	To
Incidents	Analyze alert events occurred in all managed systems.
Status	Monitors the status (Up/ Down times) of systems and applications present in an Enterprise
Behavior (An Enterprise Activity Dashboard)	Add/remove Security or Operations related enterprise activity dashlets Configure, customize, and reset Security or Operations dashlets. Generate Security or Operations volume analysis reports.
Dashboard (A Keyword Indexing Dashboard)	Add/remove Security/ Operations /Compliance related keyword indexing dashlets Configure, customize, and reset Security/ Operations /Compliance dashlets.
NetFlow	Analyze NetFlow messages collected and archived by EventTracker Direct Log Archiver.
My EventTracker	Personalize EventTracker. Only the user who has generated/configured a report/Flex reports has the permission to view them.
Change Audit	Helps to analyze voluntary and involuntary changes occurred in managed systems.
Config Assessment	Run SCAP Benchmarks against the managed systems.

Event-O-Meter

Event-O-Meter is an analytical graphical chart that helps quickly visualize per port trends of events against specified time range. In addition, numerical data has also been provided in a tabular format.

- 1 Click **Tools**, and then click **Event-O-Meter**.

Figure 13
Event-O-Meter
Graph



2 Click  at the upper-right corner to view tabular data.

Figure 14
Tabular data

The figure shows the same Event-O-Meter Graph in a Windows Internet Explorer window, but with the "Tabular data" view selected. The data is presented in a table with three columns: "Time", "514", and "14505". The table lists event counts for various time intervals, with the "14505" column showing the highest values.

Time	514	14505
5/28/2012 4:58:44 PM - 5/28/2012 5:03:44 PM	0	932
5/28/2012 5:03:44 PM - 5/28/2012 5:08:44 PM	0	996
5/28/2012 5:08:44 PM - 5/28/2012 5:13:44 PM	0	1,316
5/28/2012 5:13:44 PM - 5/28/2012 5:18:44 PM	0	990
5/28/2012 5:18:44 PM - 5/28/2012 5:23:44 PM	0	843
5/28/2012 5:23:44 PM - 5/28/2012 5:28:44 PM	0	603
5/28/2012 5:28:44 PM - 5/28/2012 5:33:44 PM	0	550
5/28/2012 5:33:44 PM - 5/28/2012 5:38:44 PM	0	484
5/28/2012 5:38:44 PM - 5/28/2012 5:43:44 PM	0	475
5/28/2012 5:43:44 PM - 5/28/2012 5:48:44 PM	0	254
5/28/2012 5:48:44 PM - 5/28/2012 5:53:44 PM	0	448
5/28/2012 5:53:44 PM - 5/28/2012 5:58:44 PM	0	409

Incorporating Your Company Logo

This option helps you incorporate your company logo into EventTracker.

To incorporate your company logo

- 1 Browse and locate 'prism.jpg' in the installation directory/images folder, typically ...\\Program Files\\Prism Microsystems\\EventTrackerWeb\\images.
- 2 Rename the "prism.jpg" image file.
- 3 Copy your company logo into that folder and then rename it as prism.jpg.
- 4 Log on to **EventTracker Enterprise**.
Find that the Prism logo at the upper-left corner is replaced with your company logo.

NOTE

The dimension should be 80 x 30 pixels.

EventTracker Components

EventVault Manager

EventVault Manager provides the capability to archive the events from the EventTracker database. The EventVault provides a simple, but important mechanism to securely archive event logs for future use and more specifically for auditing purposes.

In most enterprise networks with multiple critical servers and workstations, the event log data can become huge and unmanageable. Those event data may not be immediately required once the initial analysis is completed. At the same time they cannot be completely discarded, as they will be required for future audits. EventVault solves this problem and provides mechanisms to identify if any of the EventVault data has been tampered with.

Archives are .mdb files that are compressed into .cab files called as 'EventBox' and are stored in the **Archives** folder. If EventTracker is installed in the default path then these files could be located in the archives directory. The range of events that each EventBox contains is stored into an index file in the **Archives** folder. These EventBoxes are sorted by period and can be viewed from EventVault Manager.

To start EventVault Manager

- 1 Click the **Admin** dropdown, and then select **EventVault**.

EventTracker displays **EventVault Manager** screen.

EventVault manager stores the list of archives created. These archives can be extracted at any point of time.

Figure 15
EventVault Manager

Go to EventVault Warehouse Manager in 'EventTracker Control Panel' to change the EventVault storage location.

From	To	Name	Path	Size [KB]	Total Events	Port Number
5/30/2012 10:59:30 AM	5/30/2012 11:59:16 AM	etar1338355825-14505.cab	C:\Program Files\Prism Microsystems\EventTracker\Archives\14505\2012\5	231	3,683	14505
5/30/2012 8:59:44 AM	5/30/2012 9:59:16 AM	etar1338348650-14505.cab	C:\Program Files\Prism Microsystems\EventTracker\Archives\14505\2012\5	56	1,167	14505
5/30/2012 8:50:54 AM	5/30/2012 9:50:57 AM	etar1338352415-14505.cab	C:\Program Files\Prism Microsystems\EventTracker\Archives\14505\2012\5	33	529	14505
5/30/2012 7:59:41 AM	5/30/2012 8:59:15 AM	etar1338345034-14505.cab	C:\Program Files\Prism Microsystems\EventTracker\Archives\14505\2012\5	54	1,142	14505

Table 10

Click	To
Configuration	Configure EventVault Manager to archive the events from EventTracker database.
Verify	Verify the integrity of selected EventBoxes.
Show	View the CAB files for a specific period.

Table 11

Field	Description
From	Date & Time of the first event stored in the CAB file.
To	Date & Time of the last event stored in the CAB file.
Name	Name of the CAB file. etar1269949644-14505.cab etar – EventTracker Archive 1269949644 – Timeticks 14505 – Port number (through which the EventTracker Receiver service received the events) cab – File extension of cabinet files
Path	Path of the folder where the archives are stored typically, EventTracker install path\ port number \ year \ month
Size (KB)	Size of the CAB file in KB.
Total Events	Total number of events accommodated in the CAB file.
Port Number	Port number through which the EventTracker Receiver service received the events.

Events Knowledge Base

Knowledge Base is a repository of events whereby users can search for log-related information under one roof. KB contains carefully written articles that are kept up-to-date, an excellent information retrieval system (such as a search engine), and a carefully designed content format and classification structure.

Over a period, the KB team garnered information from various sources (Windows events, Ports, Antivirus, Veritas, Cisco PIX Firewall, Syslogs, and SNORT IDS to name a few) and uploaded on the Internet. Collecting log information is not one time job, rather perennial in nature.

Prism boasts of owning <http://kb.prismmicrosys.com> the largest repository of event data on the Internet.

EventTracker is seamlessly integrated with the Knowledge Base and provides

- Per event web reference from the Management Console based on event id and source of the event
- Suspicious Port information- This information can be downloaded from the KB to the local hard disk on per day basis. This helps to effectively monitor the suspicious network traffic

To start Events Knowledge Base

- 1 Click the **Tools** hyperlink, and then select **Knowledge Base**.

EventTracker opens website for **EventTracker KB**.

Replacing Outdated CRL

For certificate status to be determined, public key infrastructure (PKI) certificate revocation information must be made available to individuals, computers, network devices, and applications attempting to verify the validity of certificates. Traditionally, a PKI uses a distributed method of verification so that the clients do not have to contact the Certification Authority (CA) directly to validate the credentials presented. Instead, clients connect to alternate resources, such as Web servers or Lightweight Directory Access Protocol (LDAP) directories, where the CA has published its revocation information. Without checking certificates for revocation, the possibility exists that an application or user will accept credentials that have been revoked by a CA administrator.

Certificates are issued with a planned lifetime, which is defined through a validity start time and an explicit expiration date. For example, a certificate may be issued with a validity of one day, thirty years, or even longer. Once issued, a certificate becomes valid when its validity time has been reached, and it is considered valid until its expiration date. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name (for example, requiring to change the subject of a certificate due to an employee's change of name), change of association between subject and CA (for example, when an employee terminates employment with an organization),

and compromise or suspected compromise of the corresponding private key. Under such circumstances, the issuing CA needs to revoke the certificate.

There are several mechanisms to represent revocation information. RFC 3280 defines one such method. This method involves each CA periodically issuing a signed data structure called a certificate revocation list (CRL). A CRL is a list identifying revoked certificates, which is signed by a CA and made freely available at a public distribution point. The CRL has a limited validity period, and updated versions of the CRL are published when the previous CRL's validity period expires. Each revoked certificate is identified in a CRL by its certificate serial number. When certificate-enabled software uses a certificate (for example, for verifying a remote user's digital signature), the software should not only check the certificate signature and time validity, but it should also acquire a suitably recent certificate status to ensure that the certificate being presented is not revoked. Normally, a CA will automatically issue a new CRL on either a configured, regular periodic basis (for example, daily or weekly), or the CRL can be published manually by a CA administrator.

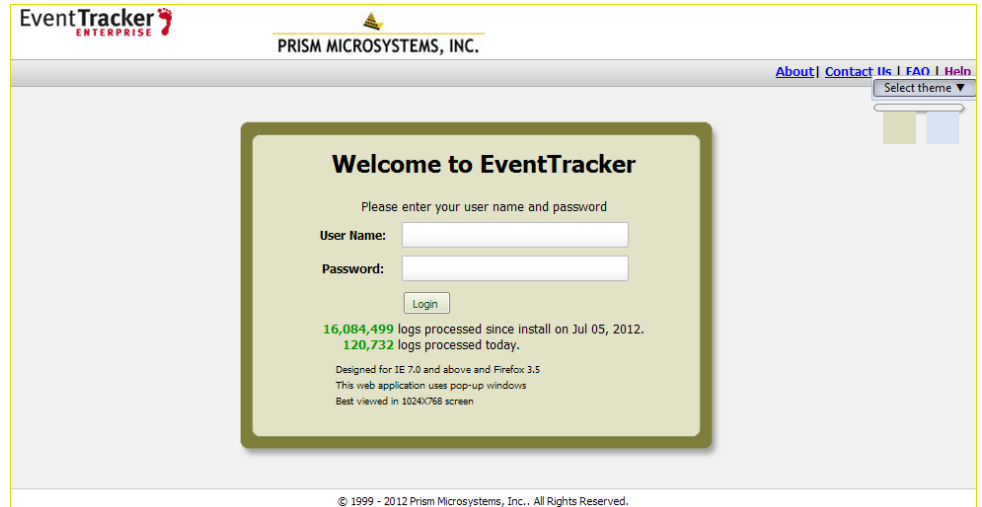
Source: <http://technet.microsoft.com/en-us/library/bb457027.aspx>

EventTracker when launched

- Verifies the validity of the Certificate
- Downloads the latest CRL published by CA.

EventTracker denies login if the validity of the certificate could not be verified or the CRL is obsolete.

Figure 16
License Verification
failed



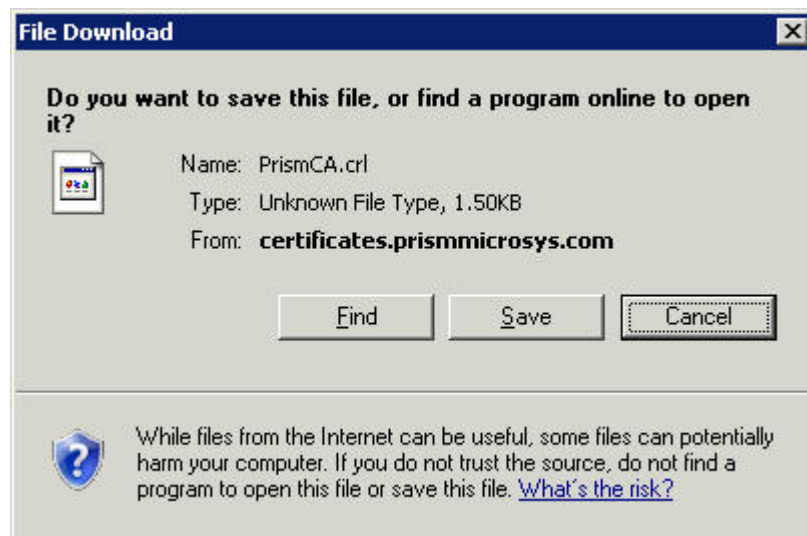
Also denies opening the Agent Configuration window on the remote agent system.

Figure 17
CRL download failed



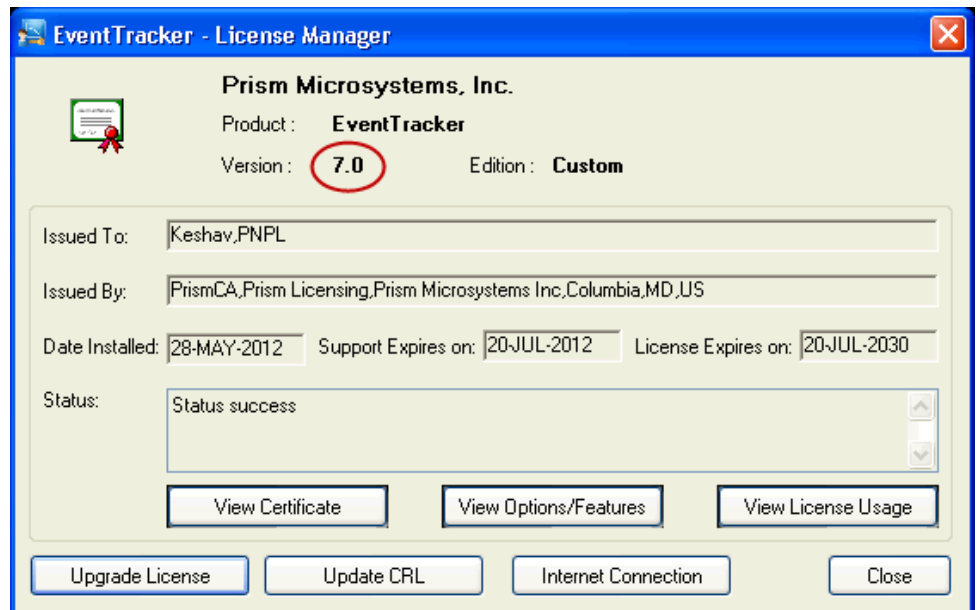
- 1 Download the latest CRL from the Web site.
File Download pop-up window is displayed.

Figure 18
CRL file download



- 2 Click **Save**.
Save As window is displayed.
Go to the appropriate folder, and then click **Save**.
- 3 Double-click **License Manager** on the **EventTracker Control Panel**.

Figure 19
License Manager



Only main version of the product will be displayed in the **License Manager** (marked in red circle). The version will not be changed with every build.

4 Click **Update CRL**.

License Manager displays the Open window.

5 Go to the folder where you have saved the downloaded CRL file and select the CRL file.

6 Click **Open**.

License Manager updates the CRL.

7 Click **Close** on the License Manager window.

8 Refresh the EventTracker Login page.

EventTracker allows you to log in.

On the remote agent system, download the CRL file to the [...\Program Files\Prism Microsystems\EventTracker\Agent folder](#).

EventTracker allows you to open the Agent Configuration window.

Updating EventTracker Users List

This option helps you update EventTracker configuration, if

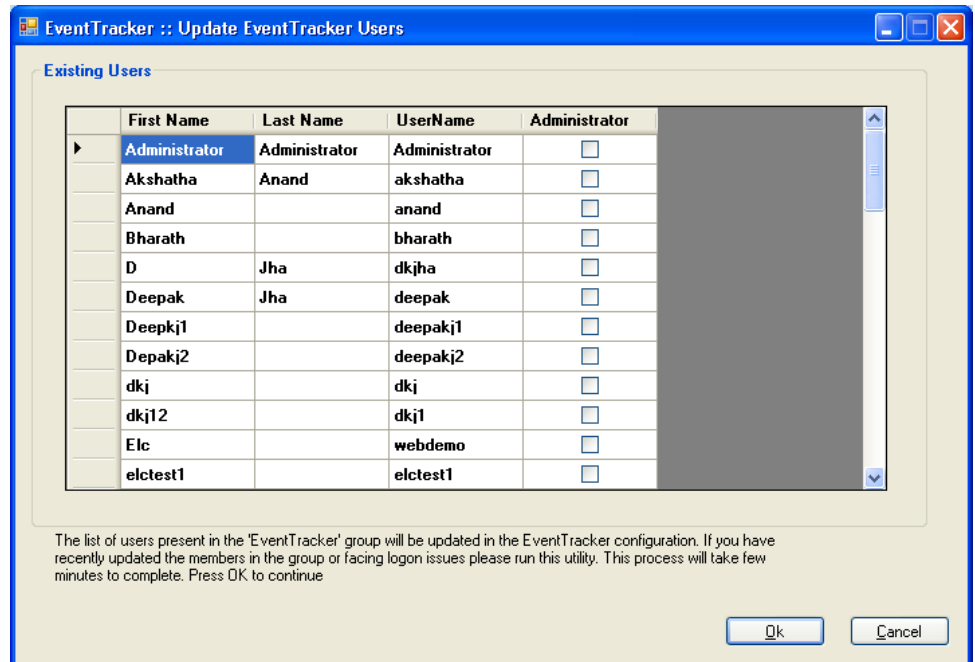
- New users are added to the "EventTracker" user group
- You face Log on issues

To update the users list

- 1 Click **Start > Programs > Prism Microsystems > EventTracker > Update Users List**.

EventTracker displays Update EventTracker Users console.

Figure 20
Update
EventTracker Users

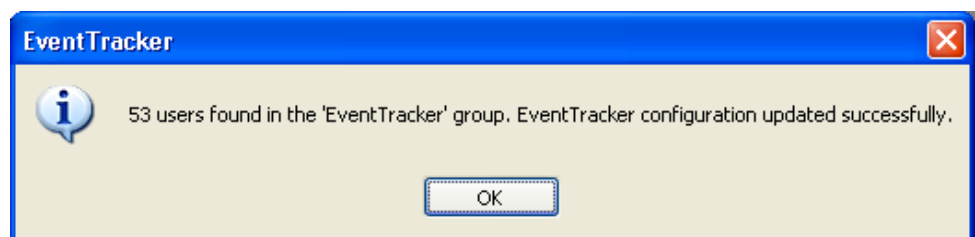


If a non-admin user is promoted as an Administrator then checkbox against the user is selected. To promote a non-admin user, refer the [Promoting a Non-Admin User as an Administrator](#) section

- 2 Click **Ok**.

EventTracker updates 'EventTracker Configuration' and displays the success message.

Figure 21
Users list updated
successfully



Exiting EventTracker

This option enables you to log out of EventTracker.

To exit EventTracker


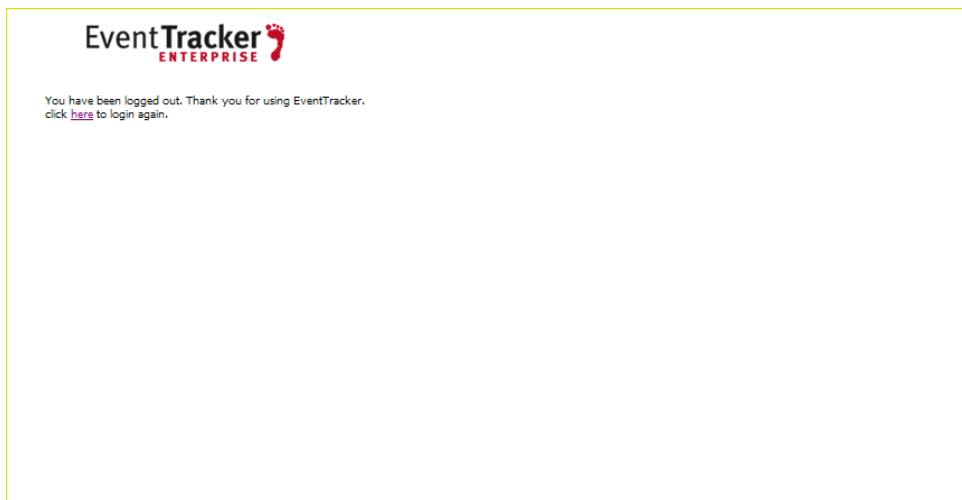
- Click the Logout icon  at the upper-right corner.
EventTracker logs you out gracefully.

Figure 22
Graceful exit



NOTE

When two users log in with the same user credentials, EventTracker logs out the first user and allows the second user to create the session.

Figure 23
Same user
credentials



 NOTE

When there is no user interaction for a specified length of time, EventTracker logs out the user.

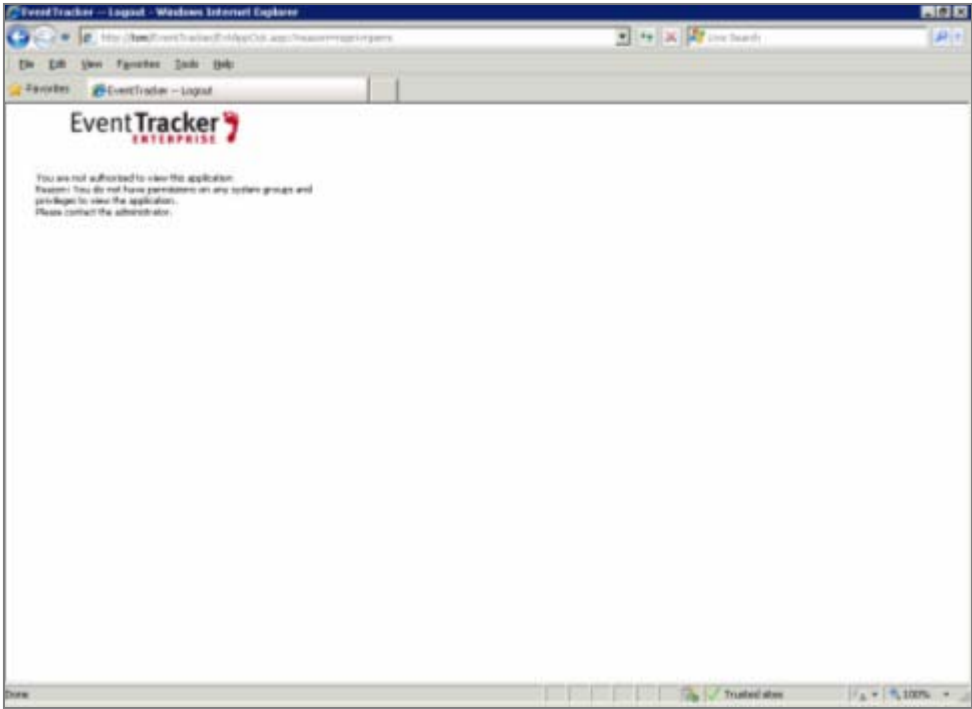
Figure 24
Session expired



 NOTE

EventTracker denies access, when a user tries to log on without appropriate access permissions and privileges.

Figure 25
Access denied



Chapter 2

Analyzing Incidents

In this chapter, you will learn how to:

- [Interpret Incidents Summary](#)
- [Search Criteria](#)

Incidents Dashboard

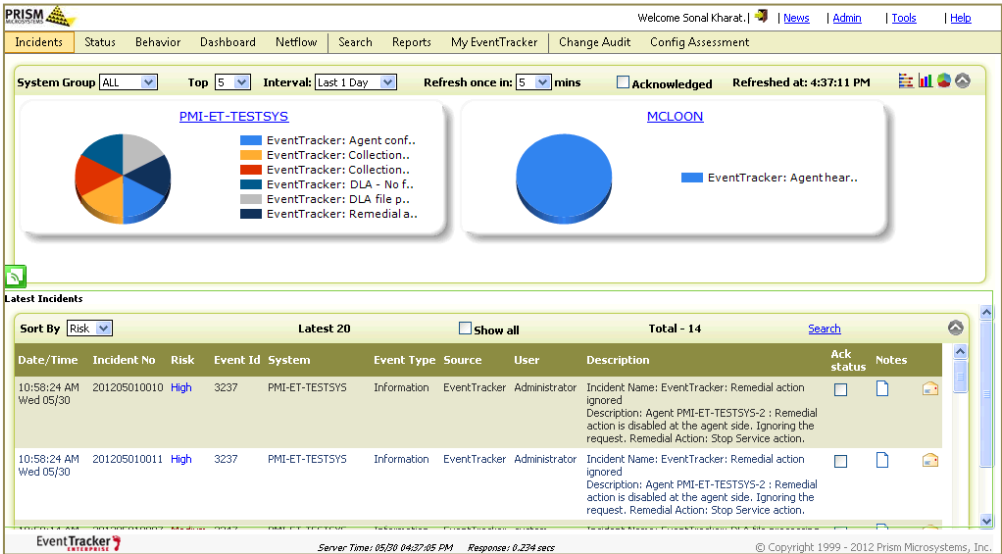
Incident dashboard helps you to interpret alert events received from managed systems. Internal scoring algorithm automatically computes and ranks alert severity levels. Only the most critical alerts that need to be attended first are displayed on the dashboard.

To analyze incidents dashboard

- Log on to **EventTracker Enterprise**.
EventTracker displays the **Incidents** dashboard containing all the unacknowledged incidents.

Figure 26
Incidents dashboard

The Incidents dashboard displays only the unacknowledged incidents, by default. To view the acknowledged incidents, click the "Acknowledged" checkbox option.



By default, EventTracker displays the incidents that are generated for past 24 hours in the managed systems. **Latest Incidents** pane will list the latest 20 incidents.





Table 12
Top pane

Incidents Dashboard – Top Pane	
Field	Description
System group	Enterprise system groups are listed in this drop-down list. By default, EventTracker selects the ALL option.
Top	By default, top 5 systems with more incidents are displayed in the top pane. You can select up to top 20 systems for displaying in the top pane.
Interval	Select the duration for which you wish to view the incident details.
Refresh once in	Set the time to refresh both the panes.
Acknowledged	Click to see the list of incidents that are acknowledged in the Latest Incidents pane. By default, the dashboard displays only the unacknowledged incidents.

Table 13
Latest Incidents Pane

Incidents Dashboard – Latest Incidents Pane	
Field	Description
Sort By	Sort Incidents list by time or risk
Show all	Click to see all the acknowledged and unacknowledged incidents occurred within specified time interval.
Search	Search incidents based on the alerts.

Table 14

Click	To
	View stacked bar graph.
	View bar graph.
	View pie graph.
	Use to expand / collapse the panes.

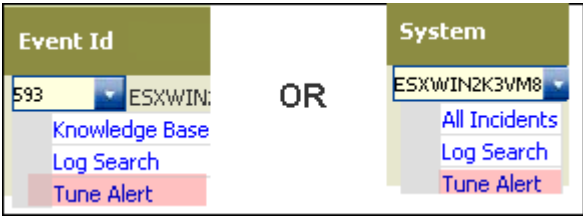
Tuning alerts configuration

This option helps you to modify alerts configuration settings. You can even activate or deactivate the alerts.

To tune alerts


- 1 Click the Event Id or system name dropdown in the bottom pane.

Figure 27
Tune Alert in context menu



From the context menu, click **Tune Alert**.

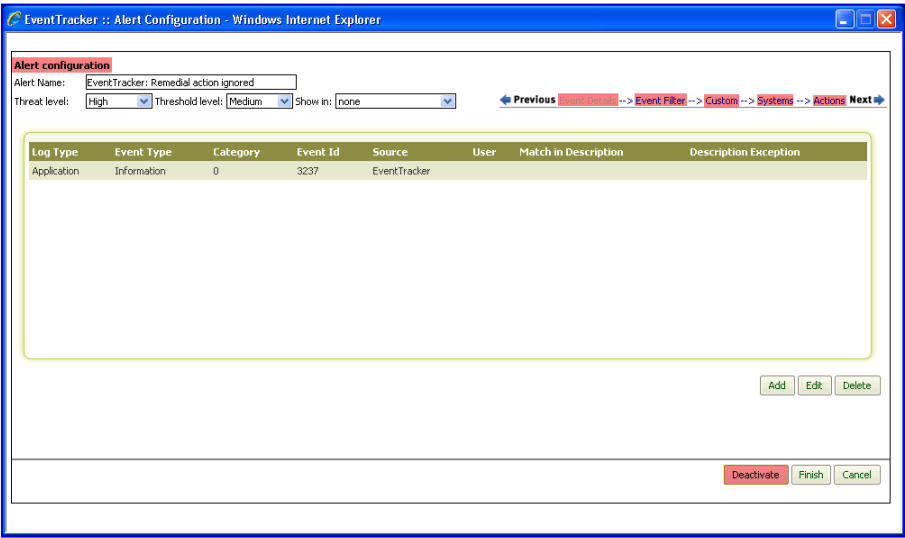
OR

In the **Search Incidents** window, click the  icon.

EventTracker displays the **Alert Configuration** -> **Event Details** page.

Figure 28
Alert Configuration
page

Tune Alerts option can be used to deactivate/edit the selected alert or to activate the deactivated alert.



- 2 Make required changes in **Event Filter**, **Custom**, **Systems**, and **Actions** pages, and then click the **Finish** button.

The modified alert configuration is saved.

NOTE

For detail information on **Alert configuration**, please read Chapter 10 - [Configuring Alerts and Alert Notifications](#).

View alert flex report

Alert flex report displays the details of total incidents occurred on a particular system.

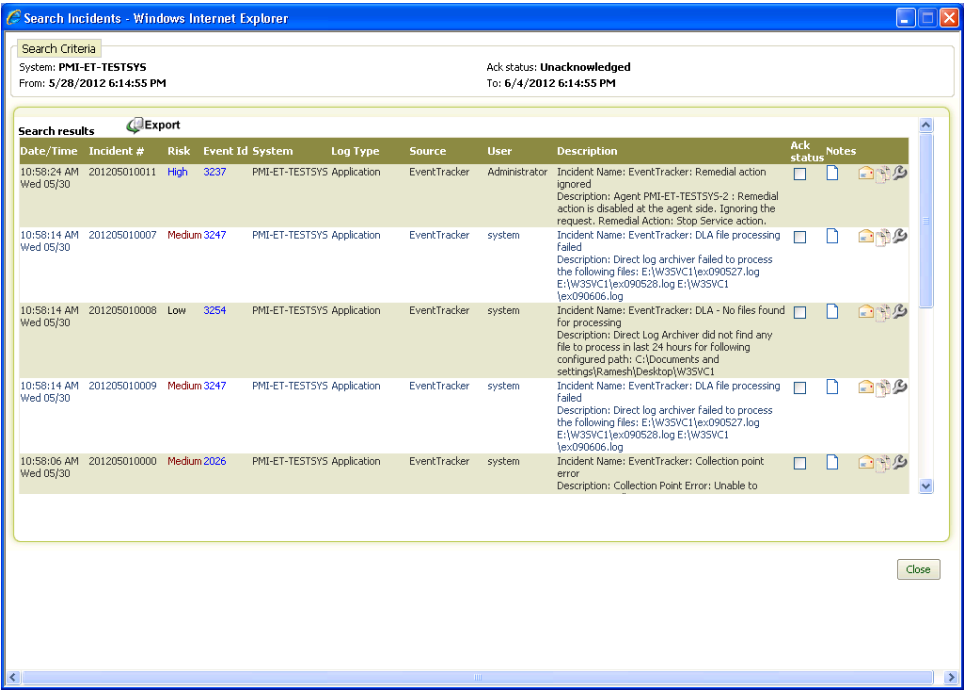
To view flex report, in the system name dropdown, click **Alert Flex Report**.

Figure 29
Alert Flex Report in
context menu



The **Search Incidents** window will appear on the screen.

Figure 30
Search Incidents
window



Log search

In **Incidents** menu, 'Log Search' feature is added to search for logs pertaining to the **System** or **Event Id**. The results obtained can further be refined.

In the **Incidents** menu- bottom pane, click **System** name or **Event ID** dropdown, and then click **Log Search**.

Log Search result window will appear on the screen.

Log Search for a **System** will display all the events related to that particular system.

Figure 31
Log Search result
window

Log search - Windows Internet Explorer

Refine Tags New search Analysis Export Total event count: 520

ID	Log Time	Event Properties	Event Description
1	6/5/2012 11:24:33 AM	Event ID: 593 Log Type: Security Event Type: Audit Success Category: 5 Source: Security Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	A process has exited: Process ID: 1988 Image File Name: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\cs.exe User Name: MCLOON\$ Domain: TOONS Logon ID: (0x0,0x3E7)
2	6/5/2012 11:24:33 AM	Event ID: 593 Log Type: Security Event Type: Audit Success Category: 5 Source: Security Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	A process has exited: Process ID: 4560 Image File Name: C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Prism.Keywo rd.Indexer.Process.exe User Name: MCLOON\$ Domain: TOONS Logon ID: (0x0,0x3E7)
3	6/5/2012 11:24:33 AM	Event ID: 593 Log Type: Security Event Type: Audit Success Category: 5 Source: Security Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	A process has exited: Process ID: 7800 Image File Name: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\cvtr.exe User Name: MCLOON\$ Domain: TOONS Logon ID: (0x0,0x3E7)
4	6/5/2012 11:24:33 AM	Event ID: 592 Log Type: Security Event Type: Audit Success Category: 5 Source: Security Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	A new process has been created: New Process ID: 7800 Image File Name: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\cvtr.exe Creator Process ID: 1988 User Name: MCLOON\$ Domain: TOONS Logon ID: (0x0,0x3E7)

Search results for: sys:MCLOON , Timerange : 6/5/2012 9:12:40 AM - 6/5/2012 11:25:12 AM

Previous Page: 1 of 52 Next Stop New search Page: 1

Log Search for an **Event ID** will display the results for the selected event Id and the system name where the event was generated.

Figure 32
Log Search result
window

Log search - Windows Internet Explorer

Refine Tags New search Analysis Export Total event count: 8

ID	Log Time	Event Properties	Event Description
1	6/5/2012 11:12:40 AM	Event ID: 2040 Log Type: Application Event Type: Information Category: 0 Source: EventTracker Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	New activity found: Event ID: 5000 System: MCLOON Time: 2012-06-05 11:07:06
2	6/5/2012 11:10:40 AM	Event ID: 2040 Log Type: Application Event Type: Information Category: 0 Source: EventTracker Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	New activity found: Process: DW20.EXE System: MCLOON Time: 2012-06-05 11:05:30
3	6/5/2012 11:10:40 AM	Event ID: 2040 Log Type: Application Event Type: Information Category: 0 Source: EventTracker Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	New activity found: Application: OFFLB.EXE System: MCLOON Time: 2012-06-05 11:05:36
4	6/5/2012 10:33:40 AM	Event ID: 2040 Log Type: Application Event Type: Information Category: 0 Source: EventTracker Domain: NT AUTHORITY Computer: MCLOON User: SYSTEM	New activity found: Network Address: ESXWIN7VM1.TOONS.LOCAL System: SAFARI Time: 2012-06-05 10:28:33

Search results for: id:2040 AND sys:MCLOON , Timerange : 6/5/2012 9:10:40 AM - 6/5/2012 11:40:28 AM

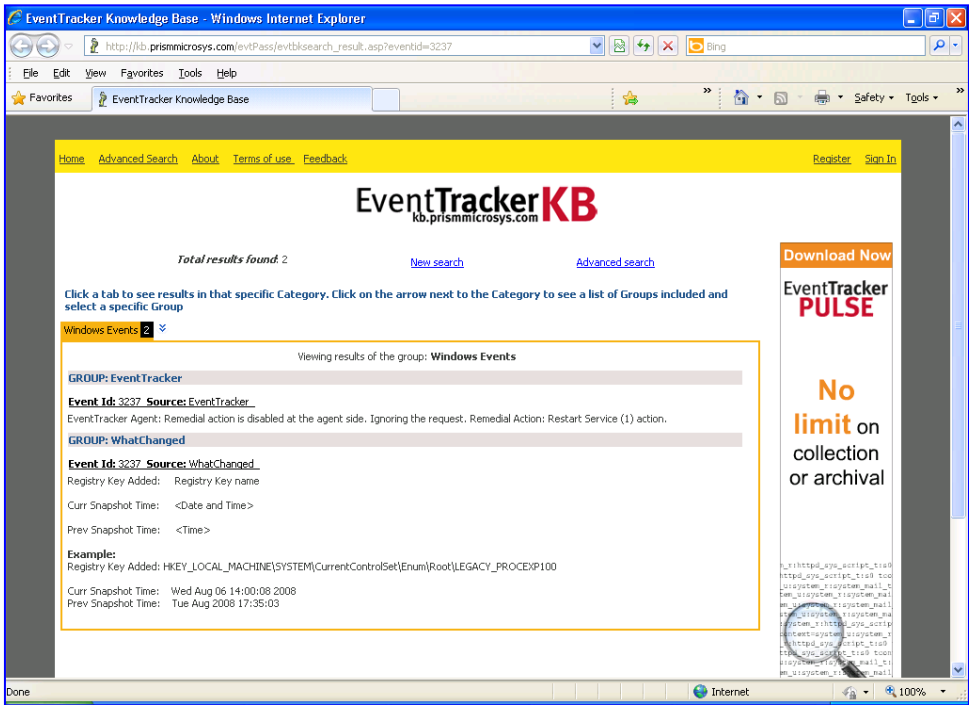
Previous Page: 1 of 1 Next Stop New search Page: 1

For more information on log search, read [Log Search](#) document.

Knowledge Base

Click **Knowledge Base** option to view event details in the 'EventTracker Knowledge Base' Web site.

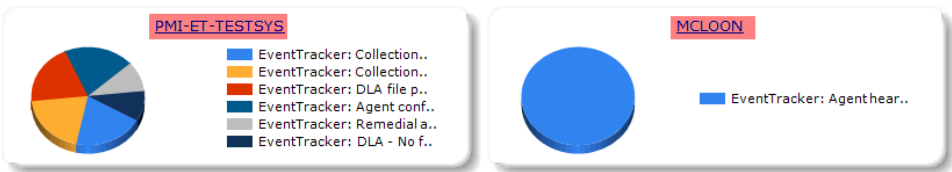
Figure 33
Knowledge Base
Web Site



'Search Incidents' window

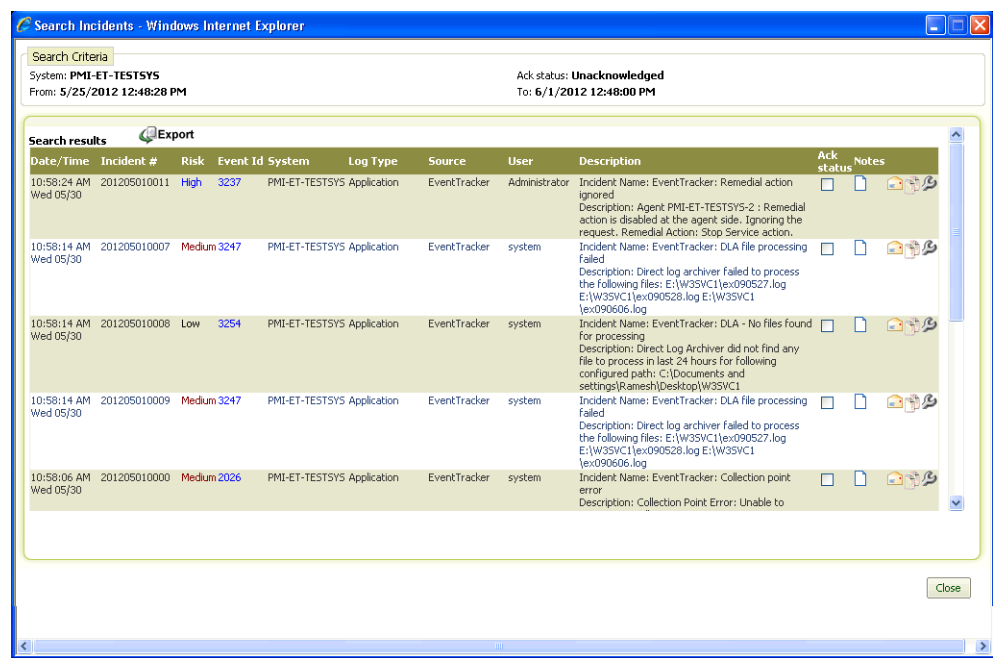
- To view the total incidents occurred on a particular system, click the system name on the 'Incidents dashboard' top pane.

Figure 34
Incidents menu-top
pane

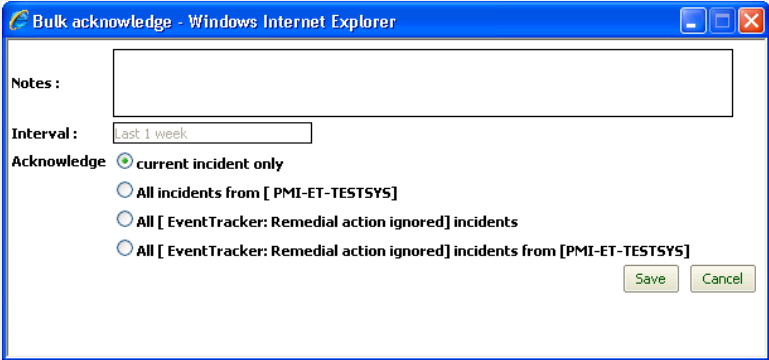

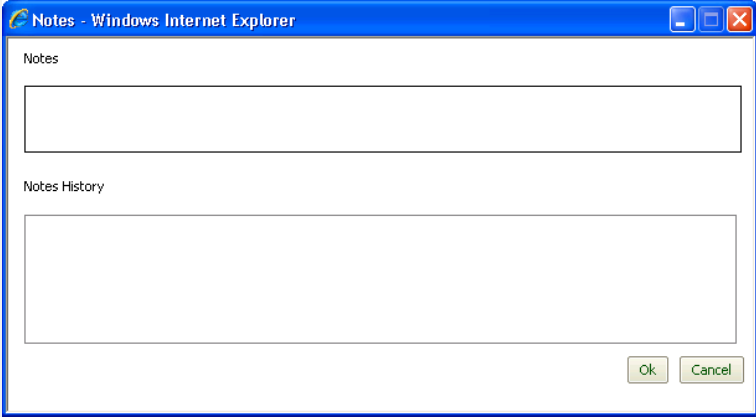



EventTracker displays the **Search Incidents** window.

Figure 35
Search Incidents



Field	Description
Date/Time	Date and time on which the incident occurred.
Incident #	A unique number assigned for each generated incident. The Incident number will be in the form of YYYYMMXXXX, where YYYY represents the year, MM represents the month, and XXXX is the auto incremented number that will be reset to 1000 on the first day of every month.
Risk	<p>Move the pointer over risk value to view vulnerability scan summary and to identify incident risk in terms of threat level, asset value, and vulnerability value.</p> <p>For example:</p> <div> <p>High</p> <div> Threat level = High Asset Value = Undefined Vulnerability = Undefined </div> </div> <p>When the vulnerability scanner(s) (ex: Nessus, Qualys) scans manager systems for vulnerability, EventTracker vulnerability parser parses the scan result file and displays the scan summary in a tooltip. This helps to quickly find the criticality of the vulnerability on the managed system(s).</p>
Event Id	Event identifier associated with the generated alert.
System	The system name where the incident occurred.
Log Type	The event/incident recorded in the following logs i.e. Application, Security, System logs.

Field	Description
Source	The source of the event. This can be the name of a program, a system component, or an individual component of a large program.
User	The user name of the user that was logged on when the incident occurred.
Description	A brief description about the incident occurred.
Ack status	<p>Check this option to acknowledge the incident. EventTracker opens Bulk Acknowledge window.</p>  <ul style="list-style-type: none"> • In the Notes pane, enter appropriate details about the action taken on the acknowledged incident. • Click appropriate Acknowledge option. The incident(s) will be acknowledged for the selected Interval. • Click the Save button to save the information.
Notes	<ul style="list-style-type: none"> • Click the Notes  icon.  <p>In Notes pane, write the comments about the particular alert or course of action taken on the alert, and then click the Ok button.</p> <p>Notes History pane will display the comments about the particular alert or action taken on the particular alert in the past.</p>
	<p>Email an incident including current Notes and Ack status. Configure the SMTP server settings to notify the incident via Email.</p>

Field	Description
 Export	Click the icon to export the incident details in 'Excel' format.

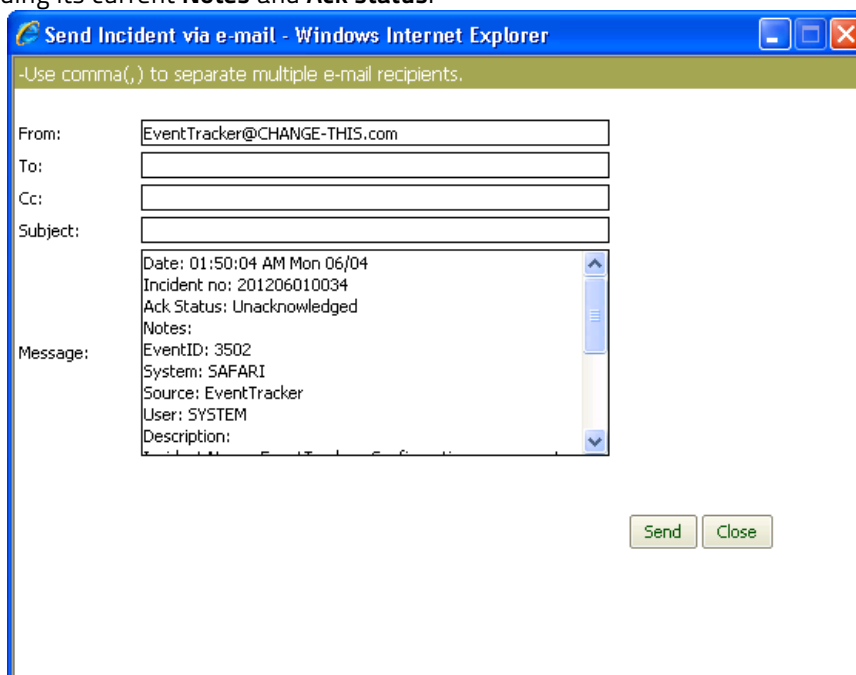
- Click any sector of pie chart/ bar of bar graph on the 'Incidents dashboard' top pane to view details of that particular Incident(s).

EventTracker will display the **Search Incidents** window that shows the detailed search results for the selected incident.

Send Incident via E-mail

In **Search Incidents** window, an option is provided to email the incident details including its current **Notes** and **Ack status**.

Figure 36
Send Incident via
email



Note that prior to this, you need to configure e-mail configuration settings under the **Admin-> Manager -> E-mail Configuration** tab.

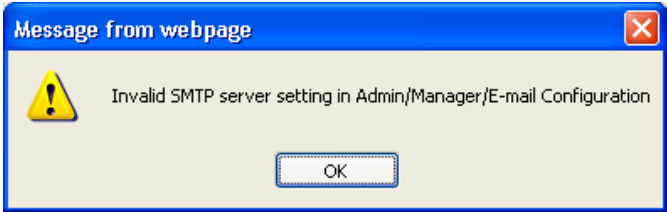
Figure 37
Manger
Configuration page

The screenshot shows the 'Manager Configuration' window with the 'E-mail Configuration' tab selected. The window contains the following fields and controls:

- SMTP server:** A text input field.
- Port:** A text input field with the value '25'.
- From e-mail:** A text input field with the value 'EventTracker@CHANGE-THIS.com'.
- To e-mail:** A text input field.
- Test E-mail:** A green button.
- Email attachment maximum size:** A text input field with the value '5' and the unit 'MB'.
- Enable authentication:** A checkbox.
- User name:** A text input field.
- Password:** A text input field.
- Save:** A green button.
- Cancel:** A green button.


If the SMTP server settings are not properly configured, then EventTracker will give an error message on attempting to send incident via Email.

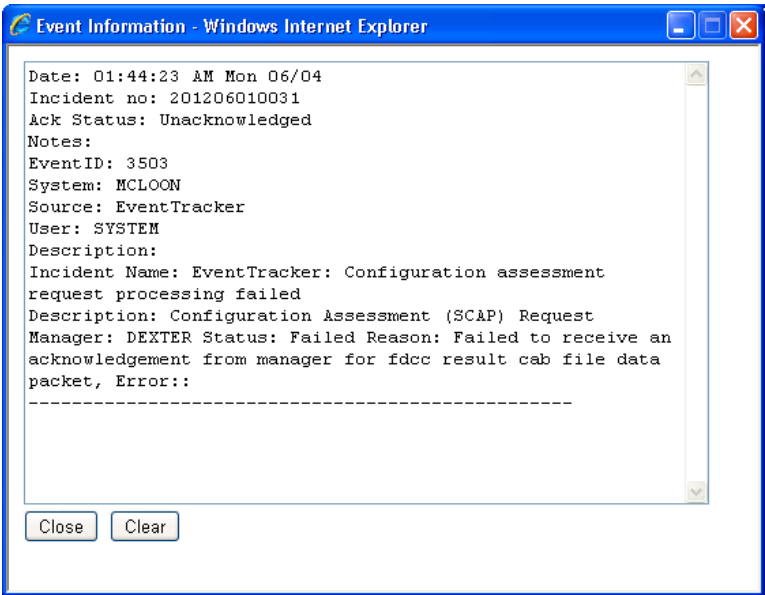
Figure 38
Error message



To get 'Event Information' in notepad

Figure 39
Event Information

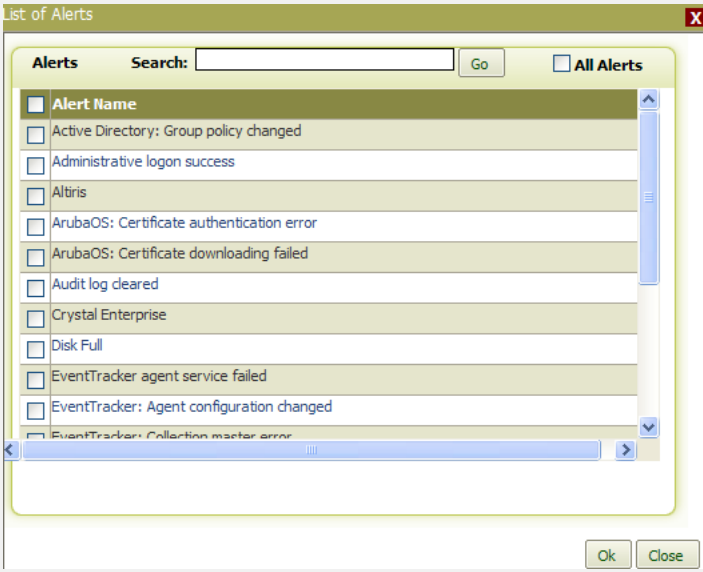
Click  icon to copy event information in the notepad.



Click the **Clear** button to clear the event information from the notepad.

Search Criteria

Search Criteria:
With The search criteria option you can search based on alert type, Risk, Incident #, Ack status, notes containing and description containing can be performed.

Search Criteria	
Field	Description
Alert / Select alert	<div>List of configured alerts with a search option and All alerts check box is provided</div> <div></div> <div>Check the required Alert name and click OK.</div>
System Select/ System	Systems search option

	<div><div><div>Systems</div><div><div>Search System(s):</div><div><div><div><div></div></div><div>tip</div></div><div><div><div><div></div></div><div>Default</div></div><div><div><div><div></div></div><div>TOONS</div></div></div></div><div><div>Ok</div><div>Close</div></div></div></div></div><div>Check the default or toons option and click OK OR Search a system name in the search option.</div></div>
Risk	<div><div>Based on event ID Risk search</div><div><div>Risk</div><div><div><div><div></div></div>Critical</div><div><div><div><div></div></div>Serious</div><div><div><div><div></div></div>High</div><div><div><div><div></div></div>Medium</div></div></div></div><div><div>Check the Risk based on the search.</div></div></div></div></div>
Duration From / to	<div><div>Based on date and time duration search.</div><div><div><div>Duration</div><div><div>From: 8/19/2012 02:13:03 PM To: 8/20/2012 02:13:03 PM</div><div><div>Search</div><div>Close</div></div></div></div></div></div>

Click	To
Incident #	Based on incident number search
Ack Status	Based on the acknowledged and unacknowledged status, search can be performed.
Notes Containing	Search based on notes
Description Containing	Search based on the event description

Web Slices

In EventTracker Enterprise, you can add latest Incidents as a Web slice.

A Web Slice is a specific portion of a webpage that you can subscribe to, and which enables you to see when updated content—such as the current temperature, or a changing auction price—is available from your favorite websites. Once you have subscribed to the Web Slice, it appears as a link on the Favorites bar. When the Web Slice is updated, the link on the Favorites bar will appear with bold formatting. You can then click the link to see the updated content.

Adding EventTracker latest incidents as Web Slice has number of advantages like,

- The latest incidents can be seen without actually logging into the EventTracker Enterprise.
- You will receive frequent notifications on the Favorites bar to view latest incidents.
- It will provide you the details of latest 20 incidents.

For more information, refer <http://windows.microsoft.com/en-GB/windows-vista/Web-Slices-frequently-asked-questions>

Adding Web Slices to the Favorites Bar

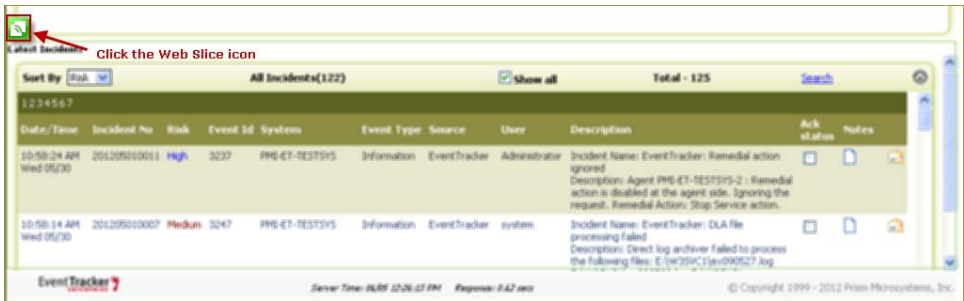
Web Slice is a web feed technology introduced in Internet Explorer 8. You need to have IE 8 to add and view Web Slices.


To add Web Slices

- 1 In the **Incidents** menu, move the mouse pointer over the bottom pane.

EventTracker displays the  (Web Slices) icon at the left hand side.

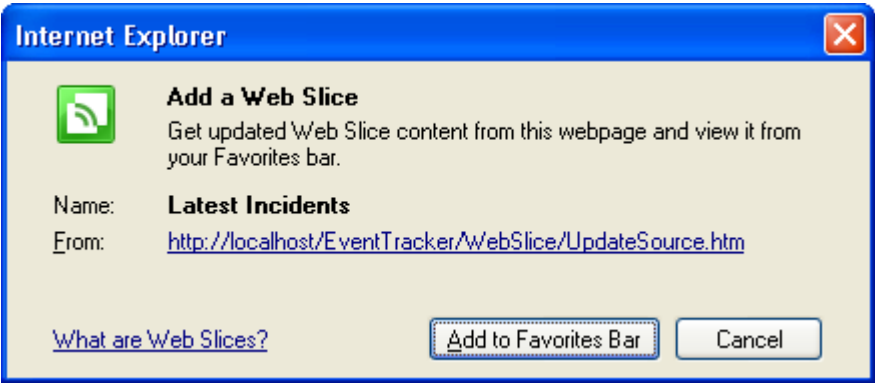
Figure 40



- 2 Click the web slice .

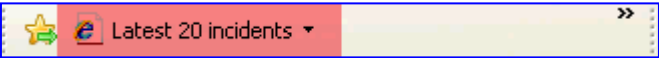
EventTracker displays the confirmation window.

Figure 41
Add a Web Slice



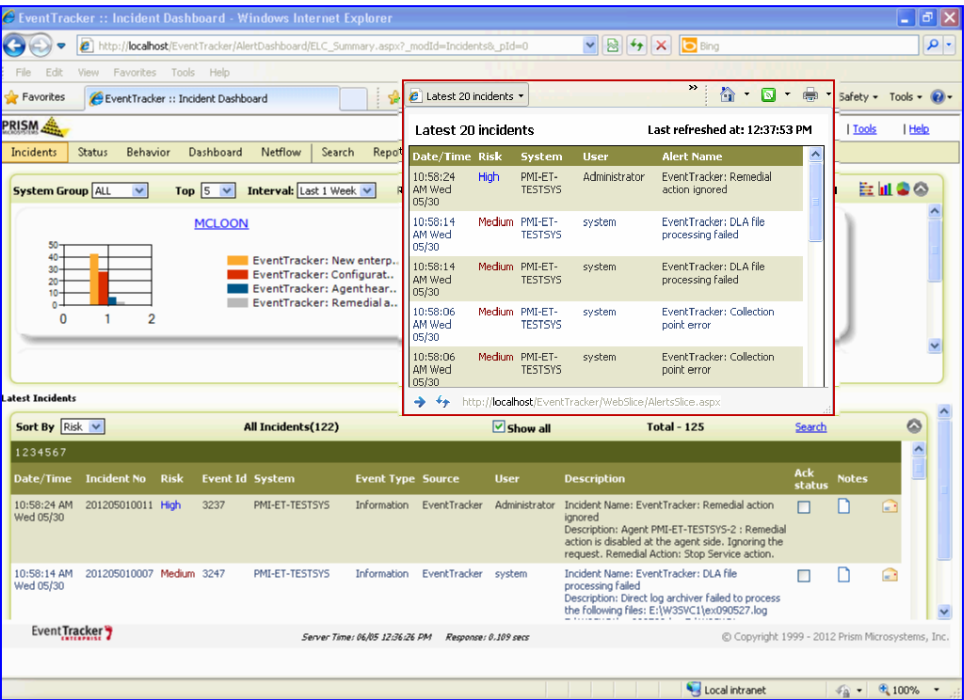
- Click **Add to Favorites Bar**.
EventTracker adds the Web Slice to the Favorites bar.
- Click the Latest 20 Incidents drop-down list on the **Favorites** bar.

Figure 42
Favorites bar



EventTracker displays the summary of top 20 Alerts.

Figure 43
Configured Web Slice



Chapter 3

StatusTracker

In this chapter, you will learn how to:

- [Create user defined group](#)
- [Add System for monitoring](#)
- [Add Application for monitoring](#)
- [Add websites for monitoring](#)
- [Remove system/application from monitoring](#)
- [View request status](#)
- [Editing Resources](#)
- [Generate Reports](#)

About Status Tracker

Status Tracker is a robust, reliable, proactive and easy to handle tool developed by Prism Microsystems, Inc. It monitors and manages the TCP/IP networks, Web sites, applications, and ports in mission critical environment with ease and comfort.

Status Tracker help users in:

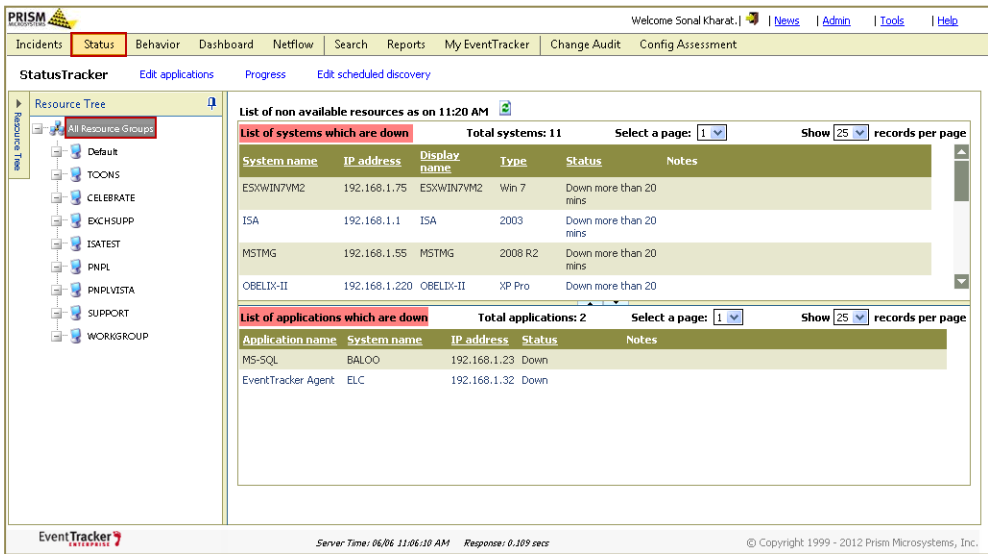
- Monitor, consolidate, generate and analyze reports about the availability status, downtime, on the TCP/IP networks configured in Windows (NT/XP/2003/VISTA/2008/2008 R2/ WIN7) platform, Web sites (http, https), applications, and ports
- Audit requirements suggested by GLBA, HIPAA, Sarbanes/Oxley, California Senate Bill 1386, the USA Patriot Act and NISPOM

StatusTracker is added in EventTracker to monitor the status of all the systems running within an enterprise and is installed on the manager server.

Getting Started with StatusTracker

- 1 Log on to **EventTracker Enterprise**.
 - 2 Click the **Status** menu.
- EventTracker displays **StatusTracker** panel.

Figure 44
StatusTracker



NOTE

All Resource Groups displays the list of systems in the top pane and applications in the bottom pane, which are currently down.

Top Pane:

Table 15
Field Description

Field	Description
System name	Name of the system which is being monitored.
IP Address	IP address of the system.
Display Name	Display name of the system.
Type	Name of the operating system
Status	Current status of the system.
Notes	Additional details regarding the system status.

Bottom Pane:

Table 16
Field Description

Field	Description
Application name	Name of the application, which is being monitored.
System name	Name of the system where the application is installed.
IP Address	IP address of the system.
Status	Current status of the application.
Notes	Additional details regarding the application status.

Sliding Pane:

Table 17
Field Description

Field	Description
Resource Tree	Contains all the default and custom groups found in the organization. The groups under resource tree can be used for add group/system/application, delete group, rename group, and remove monitoring purposes.

- 3 In the **Resource Tree** pane, click the required group name.
EventTracker displays Group details in the right pane.

Figure 45

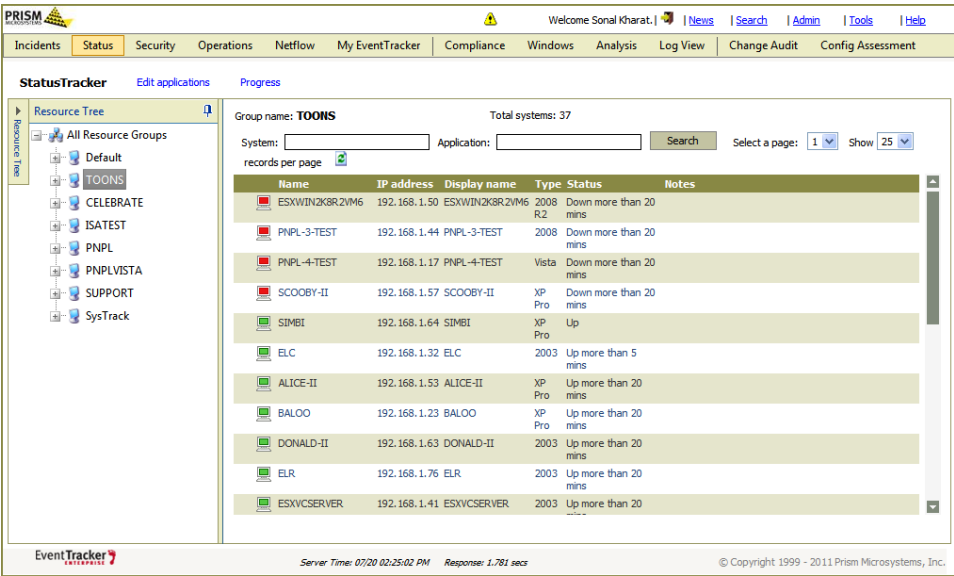














Table 18
 Convention for

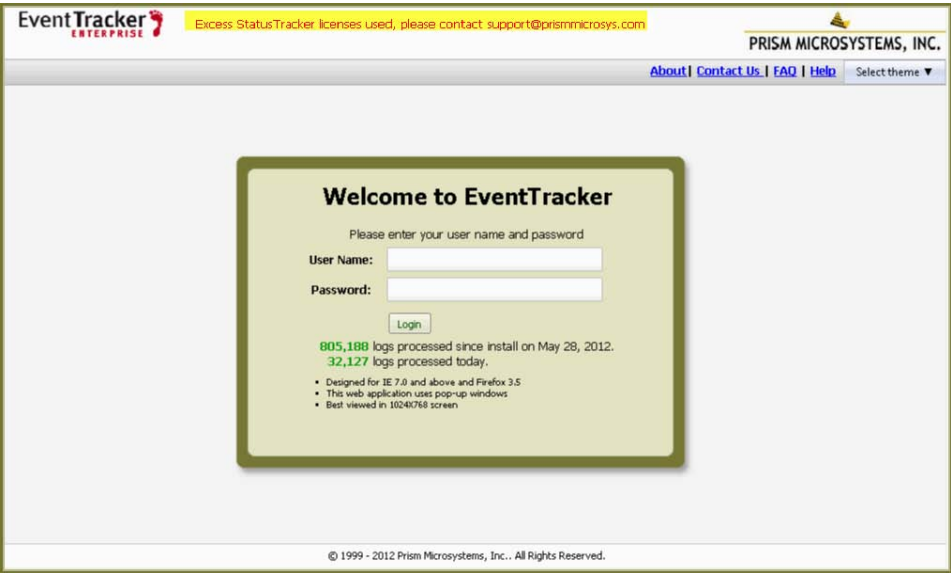
Field	Description
System	Search for system
Application	Search for application
Device Icon	Description
	System is up
	System is up but some applications in the system are down
	System is down You cannot add application to this system. If you try to add application then an error message will be displayed.
	<div> <div> <div>Message from webpage</div> <div>  <div>Applications cannot be added as the system is down</div> <div>OK</div> </div> </div> </div>
	System is kept aside for maintenance
	System is initializing
	Applications present in the system.

	Notes added for resources.
	Application is up
	Application is down
	Application is initializing

Important To Know:

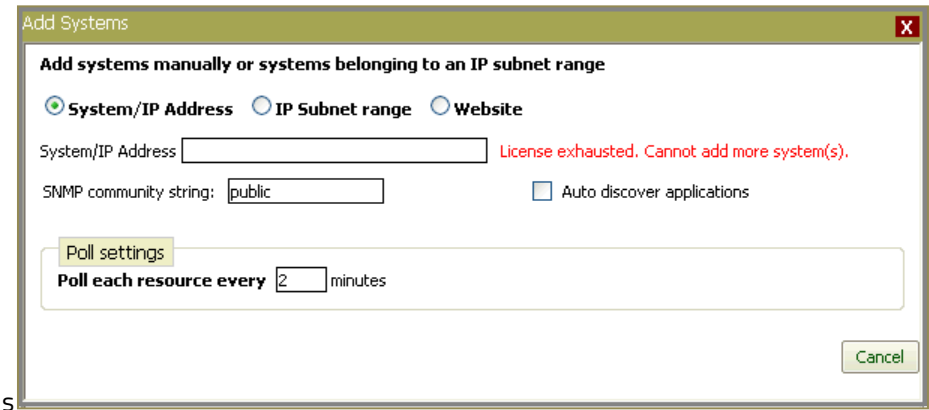
If the StatusTracker license is exhausted, then EventTracker displays an error message.

Figure 46



In addition, you cannot add more resources for monitoring if the license containing StatusTracker resources has been fully exhausted. In this case, if you try to add any system, then StatusTracker will display an error message.

Figure 47
License exhausted



Creating User Defined Group

This option helps you to select systems from different domain/group, and create a new group. Creating a user-defined group is needed when you want to monitor systems that are present in different domain/groups within the organization.

To add group

- 1 Open **StatusTracker** panel.
- 2 In 'Resource Tree' pane, right click **All Resource Groups**.
- 3 Click **Add Group**.

EventTracker displays **Add Group** pop-up window.

Figure 48
Add Group

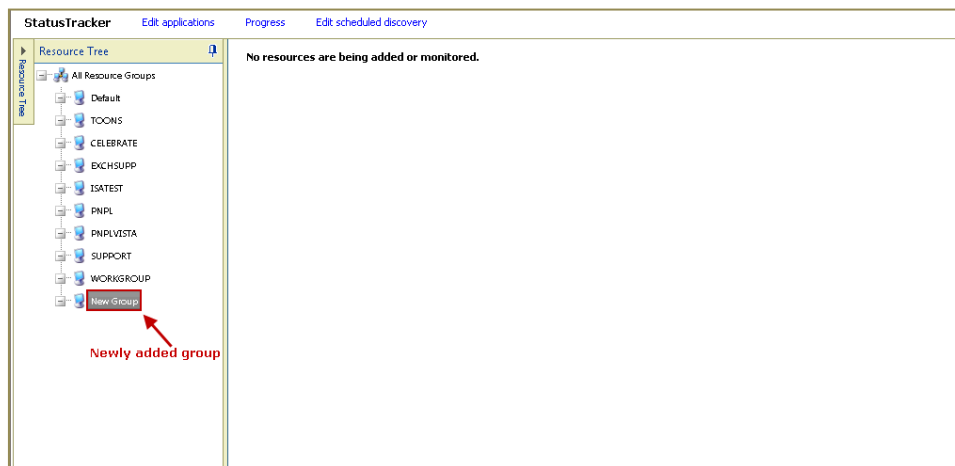


- 4 Enter appropriate group name in **Group name** box, and then click **Ok**.

For example: New Group

EventTracker displays the newly created group under resource tree pane.

Figure 49



As there are no systems/applications added in the newly created group, the right pane displays message saying '**No resources are being added or monitored**'.

NOTE

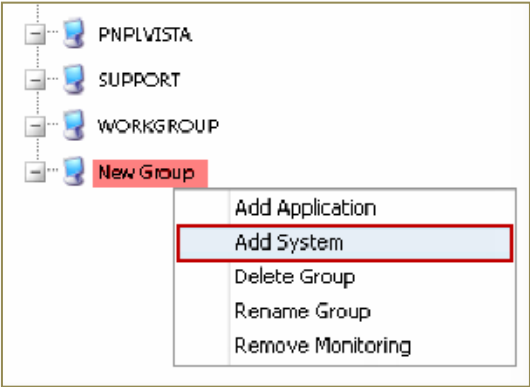
The user defined group name can be changed. To edit the group name, right click the user-defined group and select **Rename Group**. Change the group name in 'Rename Group' pop-up window, and then click **Ok**.

To add systems in the group

Once you create a user defined group, the first step is to add systems in the group.

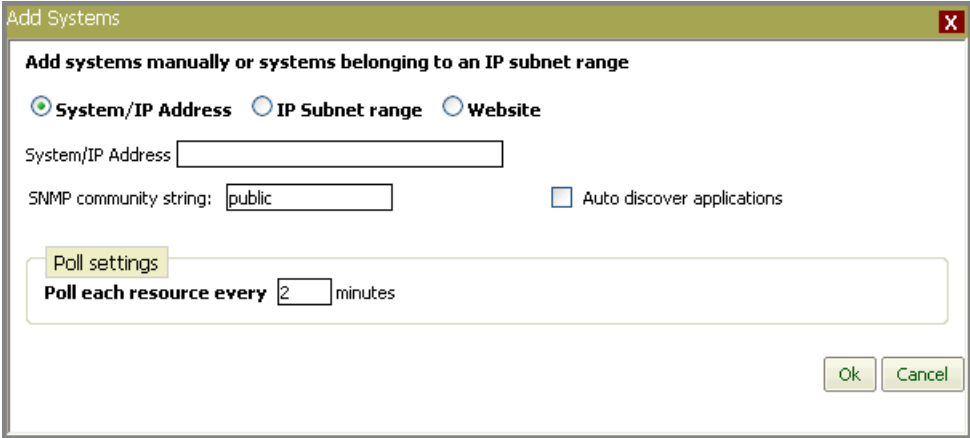
- 1 In **Resource Tree** pane, right click user-defined group.
For example: SysTrack.
EventTracker displays shortcut menu.

Figure 50



- 2 Click **Add system**.
EventTracker displays **Add Systems** pop-up window.

Figure 51
Add system/IP
address



- 3 Enter system name or IP address in the **System/IP Address** field.
For example- ELC, NEMO etc
(OR)

Select **IP subnet range** option, and then enter the IP subnet range in the **Subnet range** field.

For example- 192.168.1.1 to 192.168.1.100

Figure 52
Add IP subnet range

An SNMP community string is a text string that acts as a password. By default, SNMP Community String will be set as 'Public'. If you rename the SNMP community string, then system to be added should match the community string.

The 'Add Systems' dialog box is shown with the title bar 'Add Systems' and a close button. The main heading is 'Add systems manually or systems belonging to an IP subnet range'. There are three radio buttons: 'System/IP Address', 'IP Subnet range' (which is selected), and 'Website'. Below the radio buttons, the 'Subnet range' field is populated with '255', '255', '255', '1' followed by 'to' and '255'. The 'SNMP community string' field is set to 'public'. There is a checkbox for 'Auto discover applications'. Below that, there is a checkbox for 'Perform scheduled discovery', a 'Schedule type' dropdown set to 'Daily', a 'Week day' dropdown set to 'Sunday', and a 'Schedule time' field set to '09 : 54 : 10 : AM'. At the bottom, there is a 'Poll settings' section with a label 'Poll each resource every' followed by a field set to '2' and the word 'minutes'. 'Ok' and 'Cancel' buttons are at the bottom right.

(OR)

Select **Website** option, and then enter the Website address in the **Website** field.

For example- <http://www.eventtracker.com/>

Figure 53
Add Website

The 'Add Systems' dialog box is shown with the title bar 'Add Systems' and a close button. The main heading is 'Add systems manually or systems belonging to an IP subnet range'. There are three radio buttons: 'System/IP Address', 'IP Subnet range', and 'Website' (which is selected). Below the radio buttons, the 'Website' field is empty. At the bottom, there is a 'Poll settings' section with a label 'Poll each resource every' followed by a field set to '2' and the word 'minutes'. 'Ok' and 'Cancel' buttons are at the bottom right.

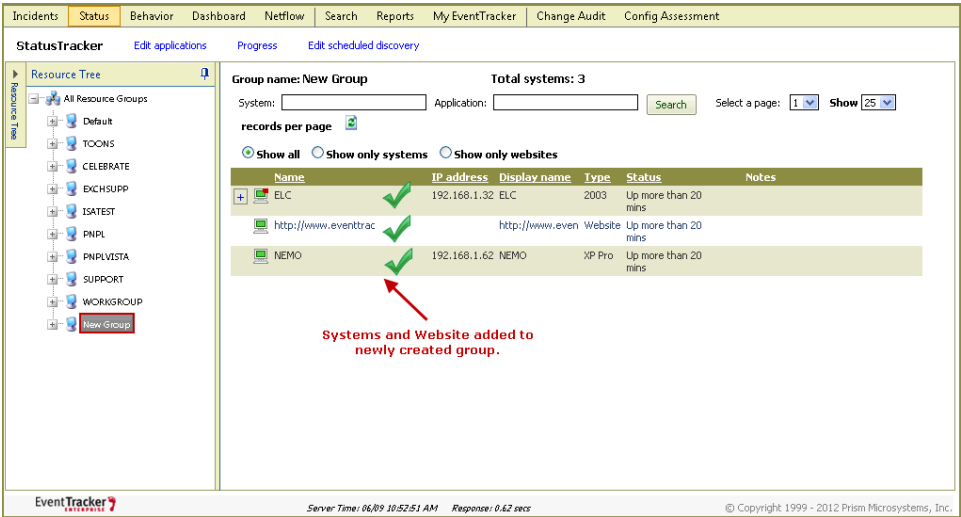
- 4 If you wish to select the default applications present in the systems then check the **Auto discover applications** option.
- 5 In **Poll Settings** pane, set the poll frequency in **Poll each resource every – minutes** field.

The default frequency is set to 2 minutes. This means, added computer will be polled/ monitored after every two minutes.

- 6 Click the **OK** button.

EventTracker displays the added systems/ IP subnet range/ Website in the right pane.

Figure 54



For example- Systems named 'ELC' and 'NEMO' and <http://www.eventtracker.com/> website added to the **New Group**.

While adding system to the group, **Auto discover applications** option was selected for 'ELC' system. Click the sign in front of the system name to see the list of applications.

- 7 Click sign to see the list of default applications present in the system.

Figure 55
List of applications
found for a system

Name	IP address	Display name	Type	Status	Notes																
ELC	192.168.1.32	ELC	2003	Up more than 20 mins																	
<table><tr><th>Application name</th><th>Port no.</th><th>Status</th><th>Notes</th></tr><tr><td> EventTracker Agent</td><td>14506</td><td>Down more than 20 mins</td><td></td></tr><tr><td> MS-SQL</td><td>1433</td><td>Up more than 20 mins</td><td></td></tr><tr><td> File Sharing, Event</td><td>139</td><td>Up more than 20 mins</td><td></td></tr></table>						Application name	Port no.	Status	Notes	EventTracker Agent	14506	Down more than 20 mins		MS-SQL	1433	Up more than 20 mins		File Sharing, Event	139	Up more than 20 mins	
Application name	Port no.	Status	Notes																		
EventTracker Agent	14506	Down more than 20 mins																			
MS-SQL	1433	Up more than 20 mins																			
File Sharing, Event	139	Up more than 20 mins																			
http://www.eventrac		http://www.even	Website	Up more than 20 mins																	
NEMO	192.168.1.62	NEMO	XP Pro	Up more than 20 mins																	

NOTE

For a system or website to be monitored in StatusTracker, ICMP should be enabled. If ICMP is disabled, systems or websites status will always appear as down.

To add application(s) for monitoring

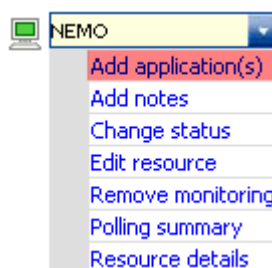
The applications present in system can be added for monitoring. Apart from the list of pre-defined applications, this option allows you to add new application(s) as well as to automatically detects all the applications present in the system.

Applications can be added to by default available group(s) as well as to the user defined group(s).

To add application(s) to a system

Using this option, you can add application(s) to an individual system.

- 1 In the **Resource Tree** pane, select the group name where the system resides for which application(s) needs to be added for monitoring.
- 2 Click the system name dropdown, and then select **Add application(s)**.



EventTracker displays **Add application** dialog box.

Add Application

Select an application from the predefined list or add a new custom application

☒ Select application ☐ New application ☐ Detect application

Host name: NEMO

Application name: Select a page:

Application name ▲	Description	Port no.
Big Brother	Big Brother System and Network Monitor	1984
Change Audit	Change Audit	14502
CMIP agent (TCP)	CMIP agent (TCP)	164
CMIP manager (TCP)	CMIP manager (TCP)	163
CMP	CMP (Certificate Management Protocol)	829
CVS	CVS version control system	2401
DHCP Manager (TCP), DNS Administration, WINS Manager, Client/Server Comm., Exchange Administrator	DHCP Manager (TCP), DNS Administration, WINS Manager, Client/Server Comm., Exchange Administrator	135
DNS	Domain Name Server	53
EventTracker Agent	EventTracker Agent	14506
File Sharing, Event Viewer, Performance Monitor, Registry Editor	File Sharing, Event Viewer, performance Monitor, registry editor	139

Poll settings

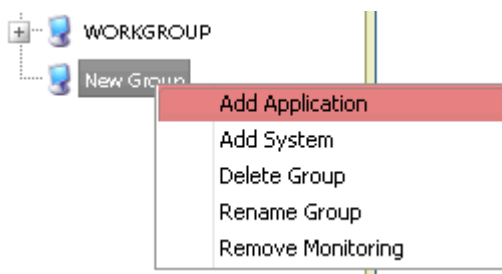
Poll each resource every minutes

- 3 Select an appropriate option to search the application.
- 4 Change the polling frequency to poll the selected application, if required.
- 5 Click the **Ok** button.

To add application(s) to more than one systems

In this option, you can select only one application at a time, but it can be added to any number of systems available under the group.

- 1 In the **Resource Tree** pane, right click the group name where application(s) needs to be added for monitoring to a number of systems, and then click **Add application**.



EventTracker displays **Add application for systems** dialog box.

Add Application for Systems

Select an application from the predefined list or add a new custom application

☒ Select application ☐ New application ☐ Detect application

Application name: Select a page: 1

Application name	Description	Port no.
Big Brother	Big Brother System and Network Monitor	1984
Change Audit	Change Audit	14502
CMIP agent (TCP)	CMIP agent (TCP)	164
CMIP manager (TCP)	CMIP manager (TCP)	163
CMP	CMP (Certificate Management Protocol)	829
CVS	CVS version control system	2401

System name: Select a page: 1

System name	Status
<input type="checkbox"/> ELC	Up more than 20 mins
<input type="checkbox"/> NEMO	Up more than 20 mins

Select the system names here to add the application(s).

Poll settings

Poll each resource every minutes

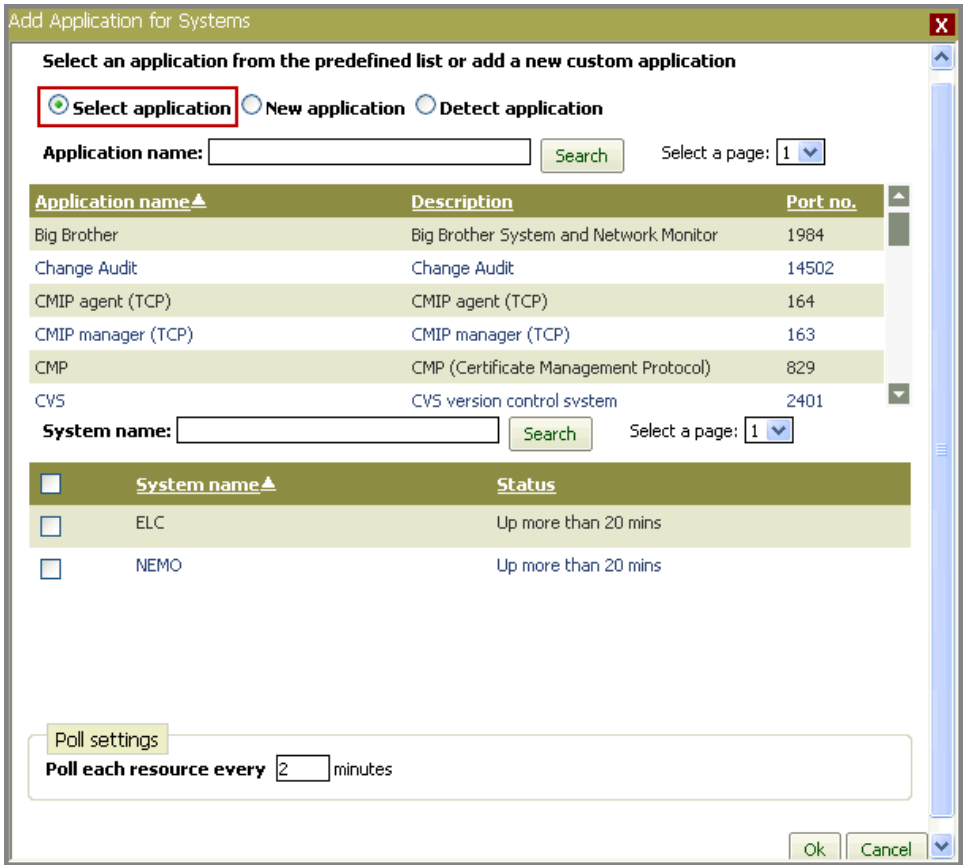
- 2 Select an appropriate option to search the application.
- 3 Check the system name(s) option to add the application.
- 4 Change the polling frequency to poll the selected application, if required.
- 5 Click the **Ok** button.

'Select application' option

You can select the application to be added from the list of predefined applications. Only one application can be selected at a time, but it can be added to any number of systems available under the group.

- 1 Click the **Select application** option, if not selected.

Figure 56
Adding existing
application for
system(s)



Add Application for Systems

Select an application from the predefined list or add a new custom application

☒ **Select application** ☐ New application ☐ Detect application

Application name: Select a page: 1

Application name▲	Description	Port no.
Big Brother	Big Brother System and Network Monitor	1984
Change Audit	Change Audit	14502
CMIP agent (TCP)	CMIP agent (TCP)	164
CMIP manager (TCP)	CMIP manager (TCP)	163
CMP	CMP (Certificate Management Protocol)	829
CVS	CVS version control system	2401

System name: Select a page: 1

<input type="checkbox"/> System name▲	Status
<input type="checkbox"/> ELC	Up more than 20 mins
<input type="checkbox"/> NEMO	Up more than 20 mins

Poll settings

Poll each resource every minutes

NOTE

Click the **Application name** or **System name** to sort the respective column.

- 2 Select the application from the list of applications in the top pane.
(OR)
Enter the application name in the **Application name** field, and then click the **Search** button.
Select the application name.
- 3 In the bottom pane, click the checkbox to select the required system for which you wish to add the selected application.

(OR)

Enter the system name in the **System name** field, and then click **Search**.

Select the system name.

(OR)

If you wish to add the selected application to all the systems present in the group, then select the checkbox in front of **System name**.

- 4 In **Poll Settings** pane, change the poll frequency for the application, if required.
- 5 Click the **OK** button.

'New application' option

- 1 Click **New application** option.

Figure 57
Adding a new
application

Add Application for Systems

Select an application from the predefined list or add a new custom application

☐ Select application
 ☒ **New application**
☐ Detect application

Application name:
 Description:
 Port:

System name:
 Select a page:

<input type="checkbox"/>	System name	Status
<input type="checkbox"/>	ELC	Up more than 20 mins
<input type="checkbox"/>	NEMO	Up more than 20 mins

Poll each resource every minutes

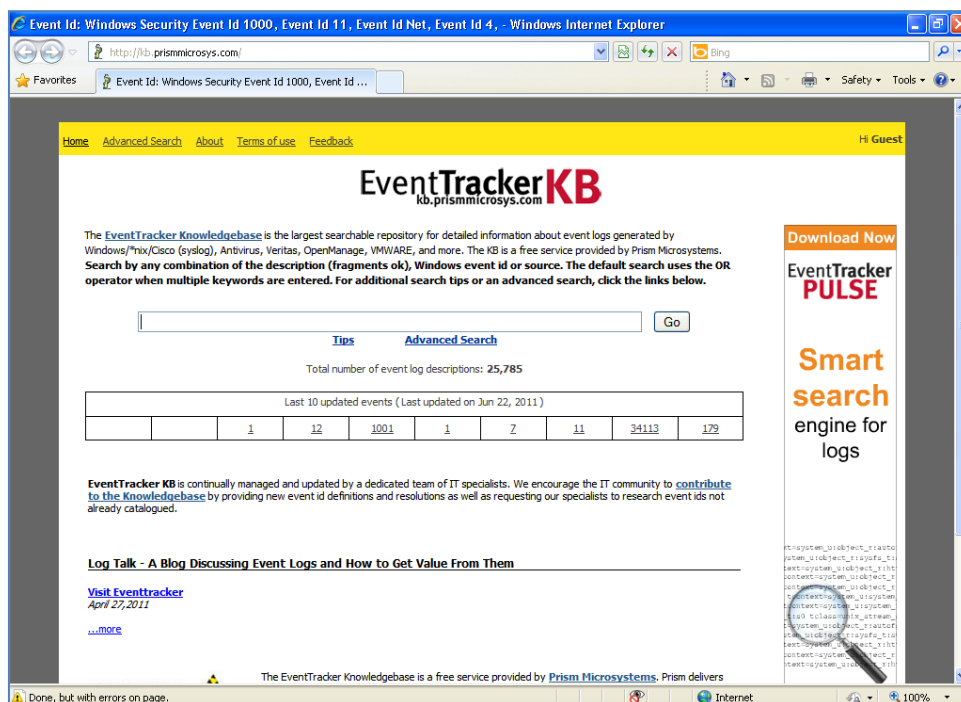
- 2 In the **Application name** field, enter the application name that you wish to add to the system(s).
 - 3 For your record, provide a brief description about the application in the **Description** field.
 - 4 Enter the valid port number in **Port** field on which the application is listening.
- (OR)

Click the **Search** button.

EventTracker opens **EventTracker Knowledge** website.

Figure 58
EventTracker
Knowledge base

Search button is provided to look out for the port numbers that are available from the EventTracker Knowledge website.



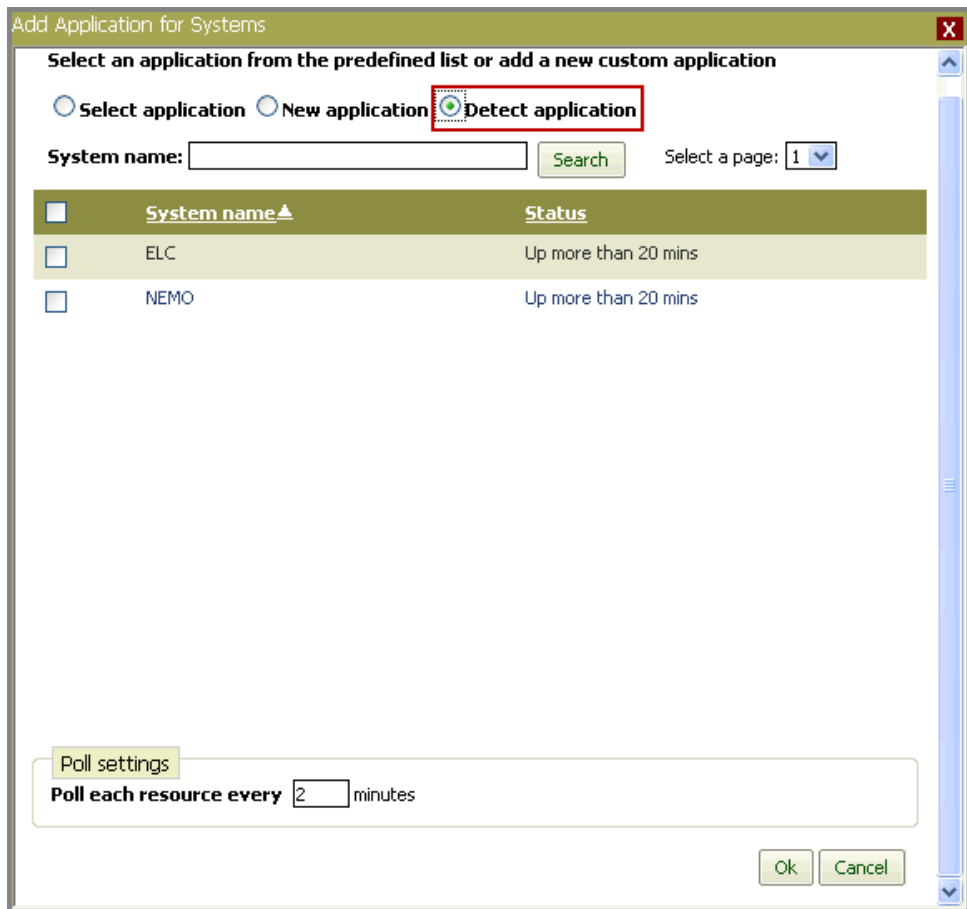
- 5 Enter the system name in **System name** field, and then click the **Search** button.
Select the system name.
(OR)
Click the checkbox to select the required system for which you wish to add the selected application.
(OR)
If you wish to add the entered application to all the systems present in the group then select the checkbox in front of **System name**.
- 6 In **Poll Settings** pane, change the poll frequency for the application, if required.
- 7 Click the **OK** button.

'Detect Application' option

This option will help you to detect all the applications present under the selected system(s).

- 1 Click **Detect application** option.

Figure 59
Detecting
applications for
system(s)



Add Application for Systems

Select an application from the predefined list or add a new custom application

☐ Select application ☐ New application ☒ Detect application

System name: Search Select a page: 1

<input type="checkbox"/> System name ▲	Status
<input type="checkbox"/> ELC	Up more than 20 mins
<input type="checkbox"/> NEMO	Up more than 20 mins

Poll settings

Poll each resource every minutes

Ok Cancel

- 2 Enter the system name in **System name** field, and then click the **Search** button.
Select the system name.
(OR)
Click the checkbox to select the required system for which you wish to detect the default application(s).
(OR)
If you wish to detect the default application(s) for all the systems present in the group then select the checkbox in front of **System name**.
- 3 In **Poll Settings** pane, change the poll frequency for the application, if required.
- 4 Click the **OK** button.

Edit Applications

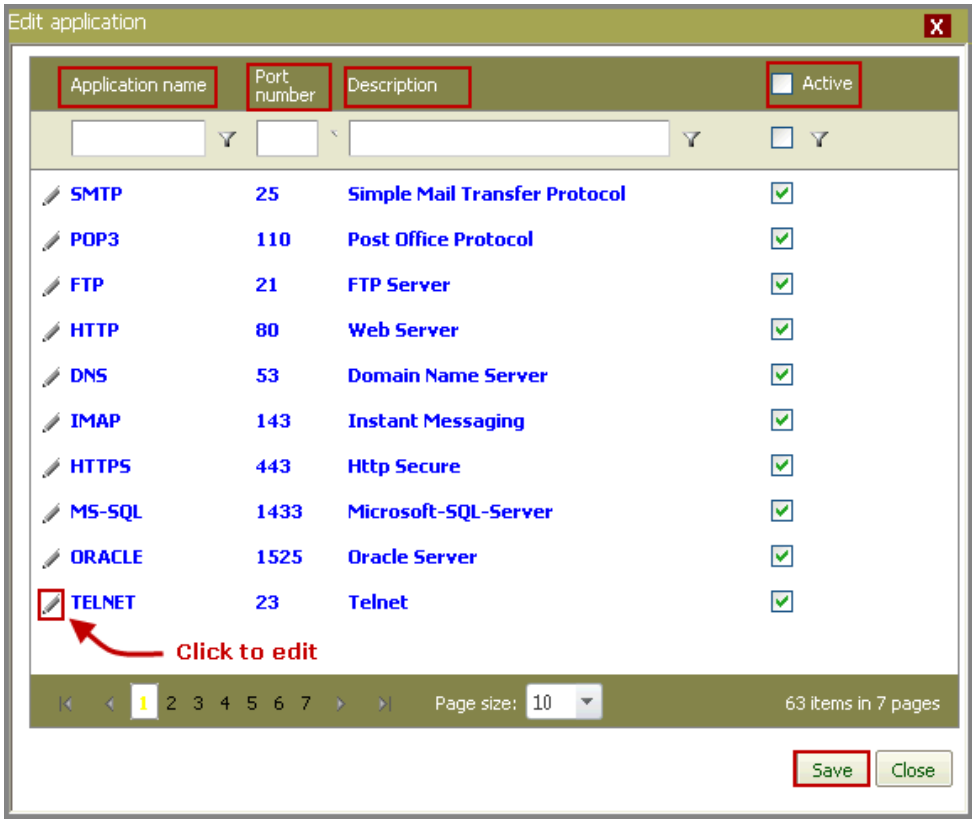
Edit Applications option is provided to modify the details of default applications. Along with the details, status of the application can also be changed from active to inactive or vice-versa.


To edit default applications

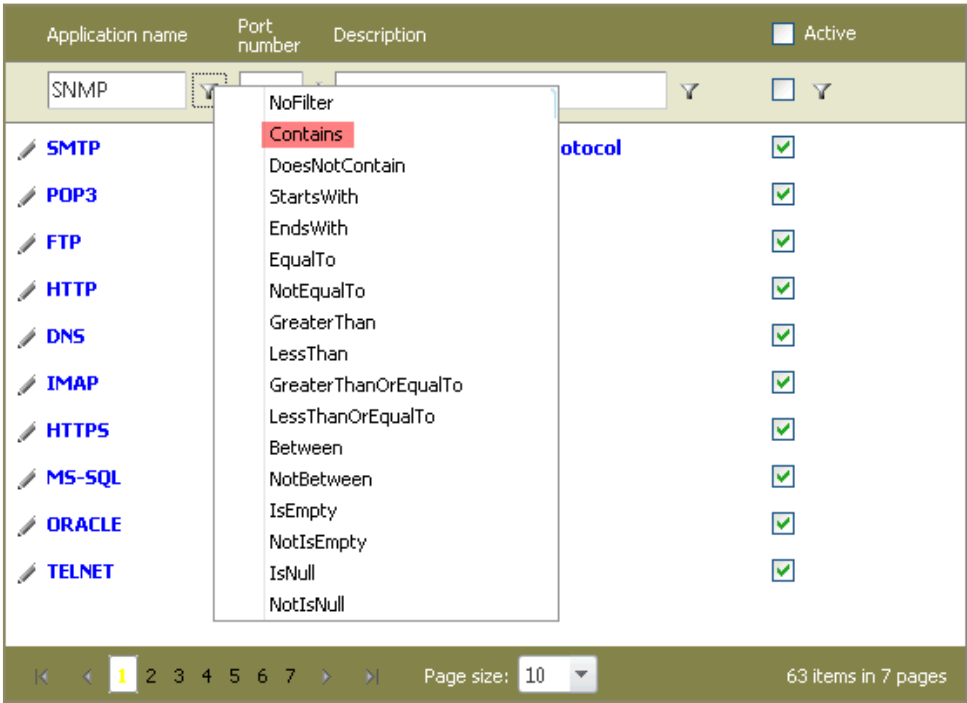
- 1 In StatusTracker panel, click the **Edit applications** hyperlink at the top left corner.

StatusTracker displays **Edit application** pop-up window.

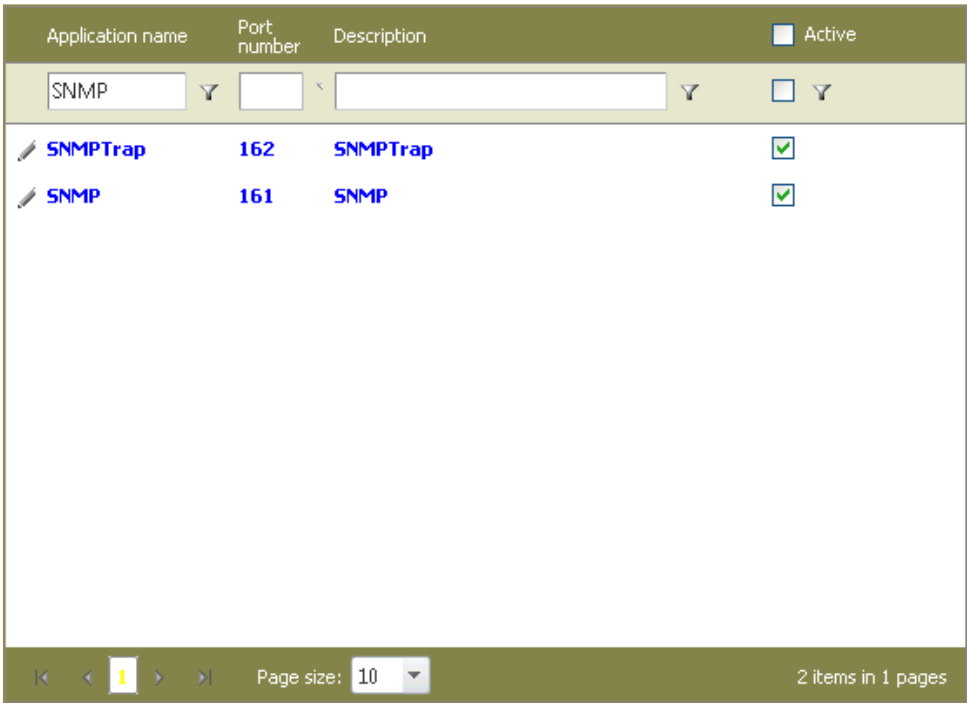
Figure 60
Edit applications



- 2 To search the application, enter the **Application name/ Port number/Description/Application status** in the respective fields.
- 3 Click the filter  icon, and then click the required filter criteria.



StatusTracker displays the search result.




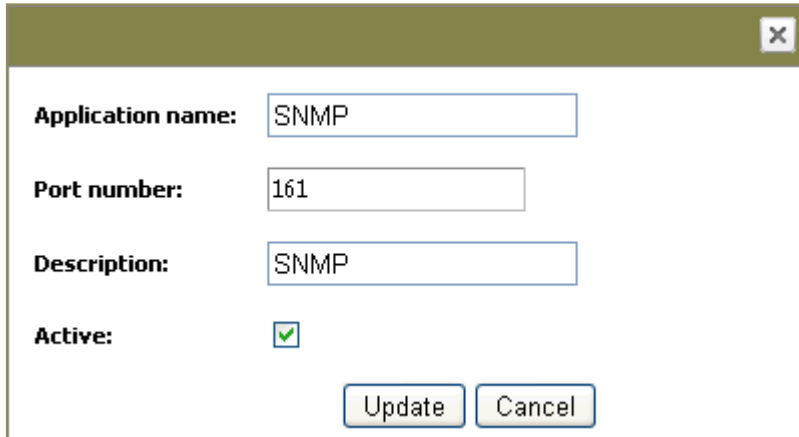
- 4 Click  icon in front of the application name to edit the application details. StatusTracker displays a dialog box.

Figure 61



The screenshot shows a dialog box titled 'Edit application' with a close button (X) in the top right corner. Inside the dialog, there are four labeled fields: 'Application name' containing 'SNMP', 'Port number' containing '161', 'Description' containing 'SNMP', and 'Active' with a checked checkbox. At the bottom right of the dialog are two buttons: 'Update' and 'Cancel'.

- 5 Edit the **Application Name**, **Port number**, and **Description** in the respective fields.
- 6 Click the **Active** checkbox to change the status of application from active to inactive and vice-versa.
- 7 Click **Update**.
- 8 In **Edit application** dialog box, click the **Save** button.
StatusTracker saves the changes made in the application.
- 9 Click the **Close** button.
Updated changes can be seen under respective applications.

View Request Status

This option will take you through list of systems/applications added along with the details. It also gives you the status of the system/application added in the group. The status can be **New** (For fresh request), **Success** (For successful addition of system/application), **Failed** (For addition of system/application failed), and **Process** (For request under process).

- 1 Open **StatusTracker**.
- 2 Click the **Progress** hyperlink at the top left corner.
StatusTracker displays **View add Systems/applications request status** pop-up window.


Figure 62
Progress status of
added system(s) &
application(s)

View add systems/ applications request status

Status: All Sort by: Date Export Refresh

Date	Group/System	By	Type	Status	Description
6/9/2012 11:14:24 AM	http://www.google.co.in/	Sonal	Add systems	Success	Success
6/9/2012 10:52:51 AM	ELC	Sonal	Add systems	Success	success
6/9/2012 10:52:25 AM	NEMO	Sonal	Add systems	Success	success
6/9/2012 10:49:56 AM	http://www.eventtracker.com/	Sonal	Add systems	Success	Success
6/9/2012 10:15:52 AM	sherkhan	Sonal	Add systems	Success	success
6/7/2012 2:51:54 PM	simbi	Sonal	Add systems	Success	success
6/7/2012 2:44:14 PM	jerry	Sonal	Add systems	Success	success
6/7/2012 2:38:23 PM	simbi	Sonal	Add systems	Success	success
6/7/2012 2:31:30 PM	leo	Sonal	Add systems	Success	success
6/7/2012 11:48:04 AM	safari	Sonal	Add systems	Failed	failed
6/7/2012 11:47:05 AM	Webdoc2	Sonal	Add systems	Failed	failed

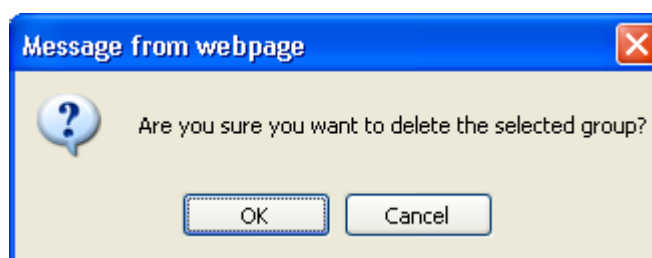
Close

- Click refresh  button to get the updated status.
 - Use the **Status** dropdown, to see the specific status progress.
 - Sort the activities by date/system/type/status in the **Sort by** dropdown.
 - Click **Export** to export the status details in the excel sheet.

Delete Group

Figure 63
Delete group
confirmation

Only user defined groups can be deleted. The default groups cannot be deleted.



- Click **OK**.
All the systems and applications will be moved into the 'Default' group (EventTracker defined group).

 **NOTE**

The systems and applications will be moved from user-defined group to the 'Default' group, but the resources will continue to be monitored as before. Only the mapping with the current group is removed.

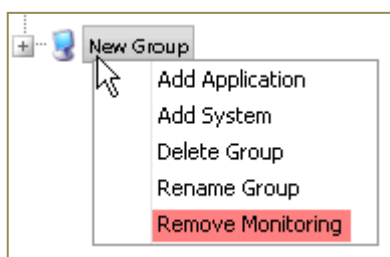
Remove Monitoring

You can remove number of systems or Websites from monitoring present in a group and also can choose a single system to remove from monitoring.

To remove multiple systems/Websites from monitoring

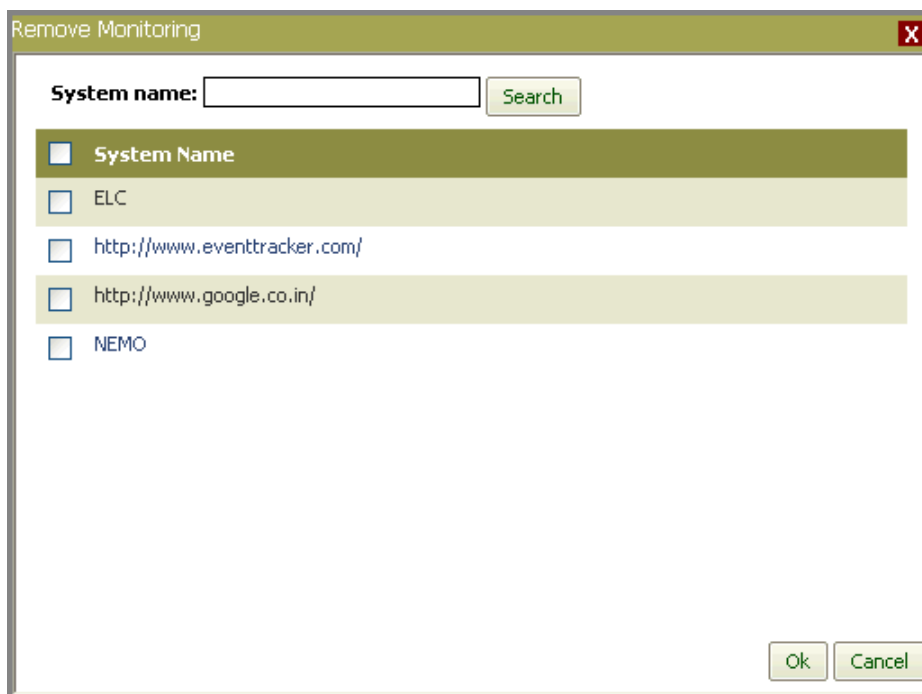
- 1 Right click the group name where system(s) or Website(s) to be removed from monitoring is present, and then click **Remove monitoring**.

Figure 64



StatusTracker displays **Remove monitoring** pop-up window.

Figure 65
Remove system(s)
from monitoring



Remove monitoring dialog box displays all the systems and Websites belonging to the selected group.

- 2 To remove individual system/Website from monitoring, click the checkbox in front of the required system/Website name.

(OR)

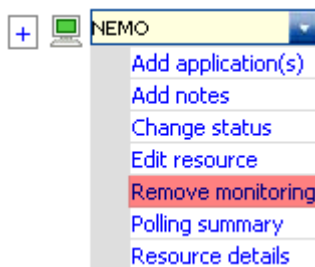
To remove all the systems from monitoring, click the checkbox in front of **System Name**.

- 3 Click the **OK** button.

To remove a system/Website from monitoring

- 1 Click the system/application name dropdown, and click **Remove monitoring**.

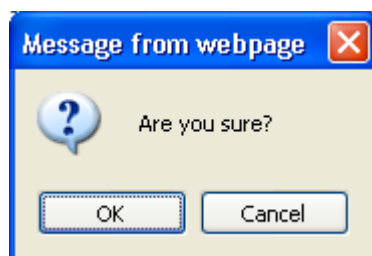
Figure 66



StatusTracker displays confirmation message.

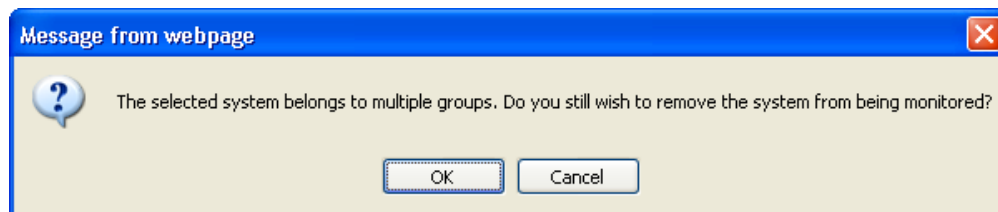
For user defined group- systems and applications:

Figure 67



For EventTracker defined group- systems and applications:

Figure 68



- 2 Click **OK**.

NOTE

If a system in user-defined group is removed from monitoring, then it will also be deleted from the default group.

Add removed systems for monitoring

This option helps you to restart the system monitoring service.

- 1 Click the **Admin** dropdown, and then select **Systems**.
- 2 Right click the group name where systems to be added is present and select **Add systems for monitoring**.

Figure 69
System Manager

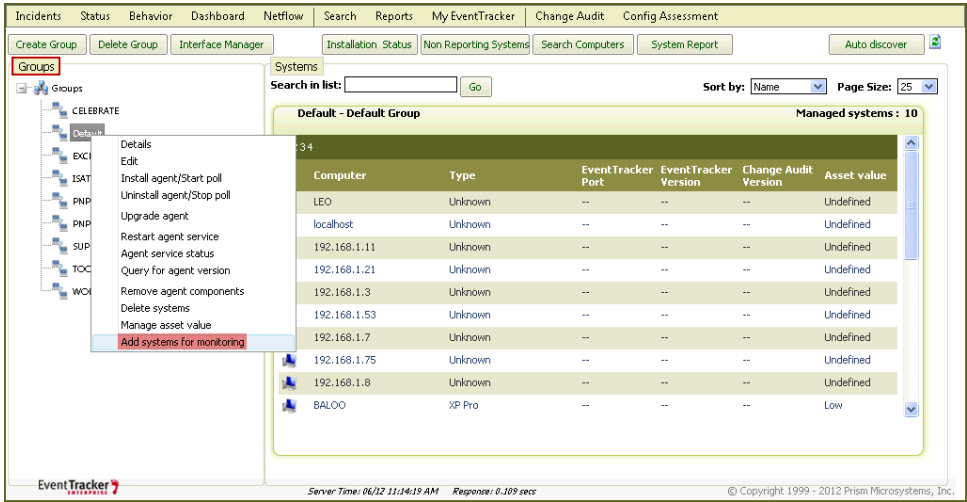
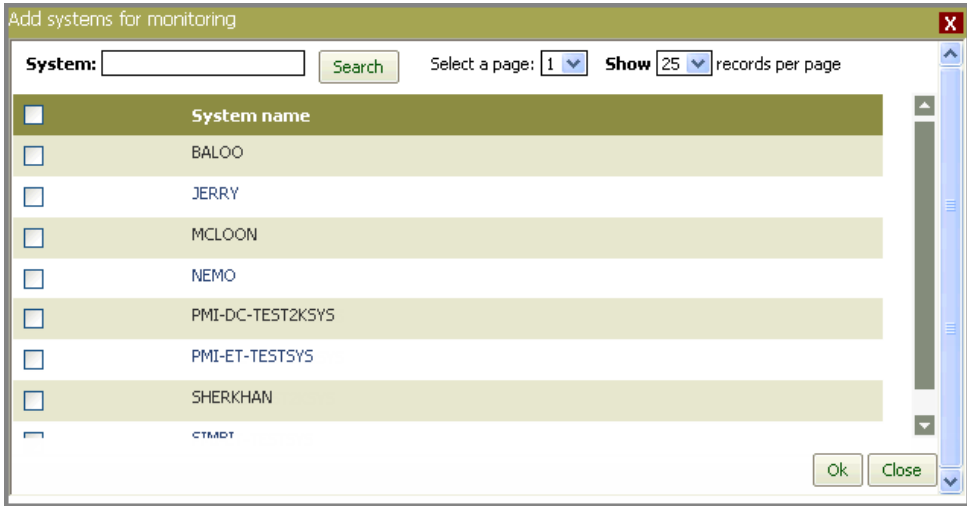


Figure 70
Add system for
monitoring

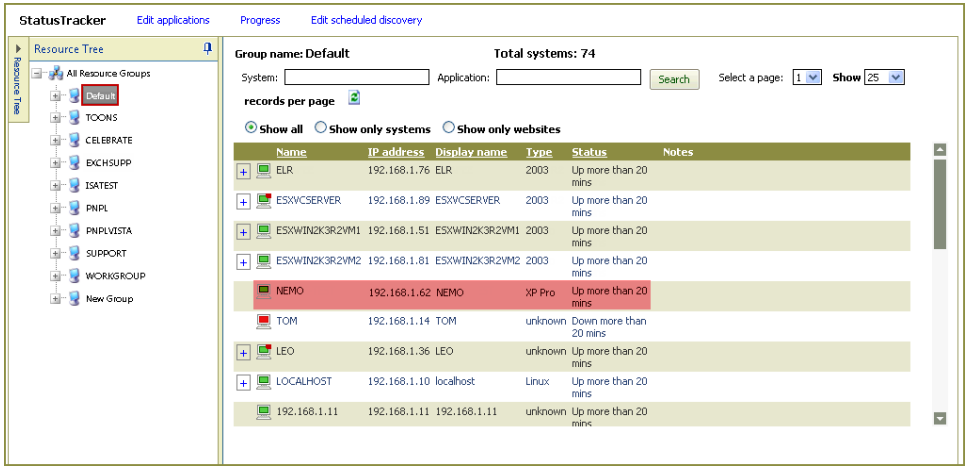
EventTracker displays **Add systems for monitoring** dialog box.



- 3 Enter the system name which is to be added for monitoring in **System** Field, and then click the **Search** button.
- 4 Select the checkbox in front of the system name, and then click the **Ok** button.
Selected system(s) should be added in the StatusTracker. Go to StatusTracker menu for verification.
- 5 Click the **Status** menu.
- 6 In the **Resource tree** pane, select the group name to which you have added the system for monitoring.

StatusTracker displays the list of systems belonging to the group.

Figure 71



StatusTracker also lists the system name which you have added earlier for monitoring from **System** manager.

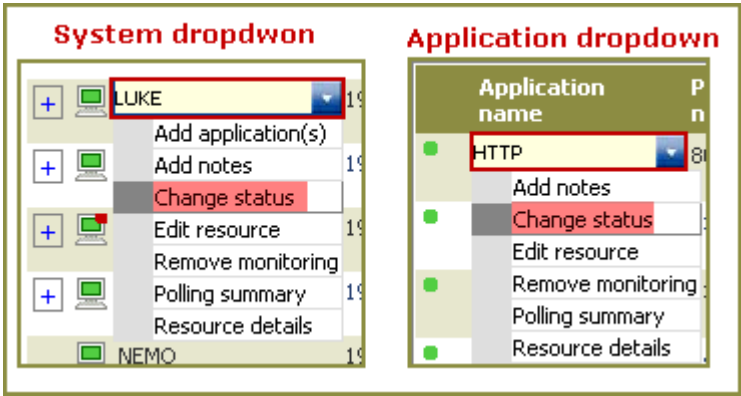
Change Status

This option can be used to temporarily put the system or application out of monitoring. You can change the system/application status from up/down to maintenance and from maintenance to up.

To change the System/Application status to 'Maintenance'

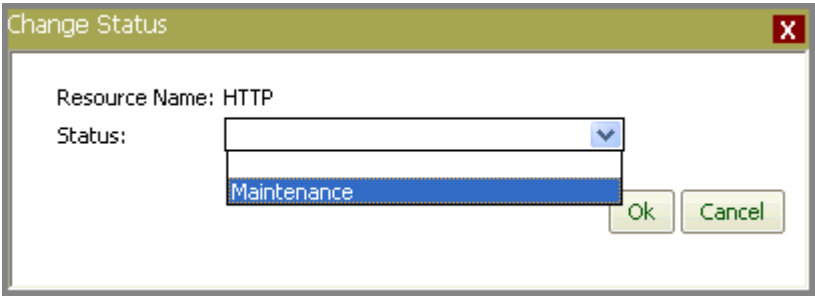
- 1 Click the system name/application name dropdown, and click **Change Status**.

Figure 72



StatusTracker displays **Change Status** window.

Figure 73
Change Status to
'Maintenance'



- 2 Click 'Maintenance' from the **Status** dropdown, and then click **Ok**.
StatusTracker page displays the system or application status as maintenance.

Figure 74
System status

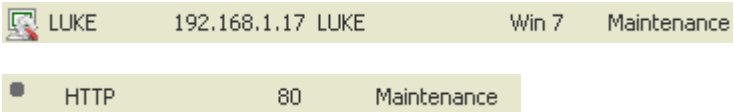


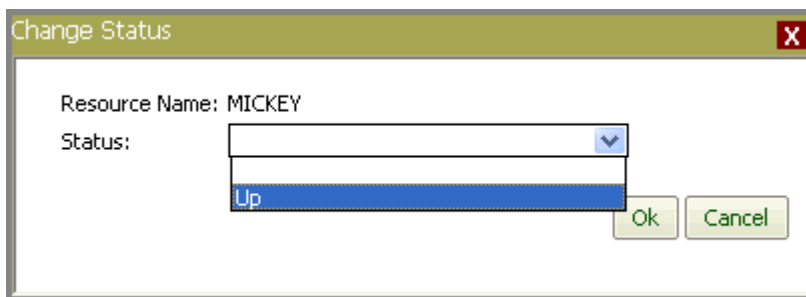
Figure 75
Application status

The 'Maintenance' status needs to be updated manually to 'Up'. The status will not get changed automatically from 'Maintenance' to 'Up'.

To change 'Maintenance' status

- 1 Select the system/application, which is under 'Maintenance' status, and then click the dropdown menu.
- 2 Click **Change Status**.
StatusTracker displays 'Change Status' window.
- 3 In **Status** dropdown, change the status to **Up**, and then click the **OK** button.

Figure 76
Change status to
'Up'



A dialog box titled "Change Status" with a close button (X) in the top right corner. It contains the text "Resource Name: MICKEY" and a label "Status:" followed by a dropdown menu. The dropdown menu is open, showing "Up" as the selected option. At the bottom right, there are "Ok" and "Cancel" buttons.

NOTE

The system or application status cannot be changed from maintenance to down. You can use 'Change Status' option to temporarily put the system/application out of monitoring.

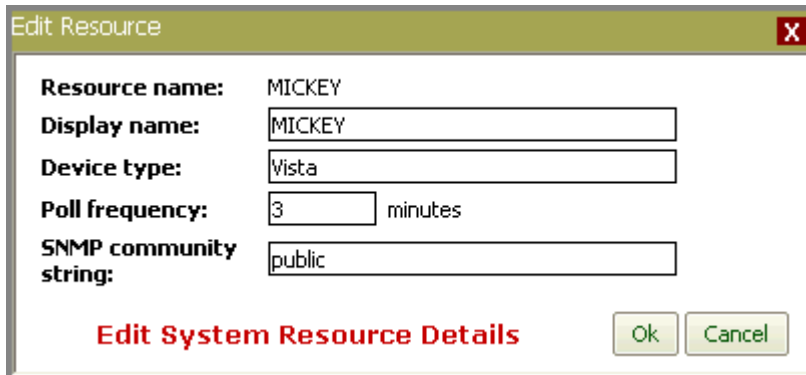
Edit Resources

The system or application resource details can be changed for identification purpose.

To edit resources

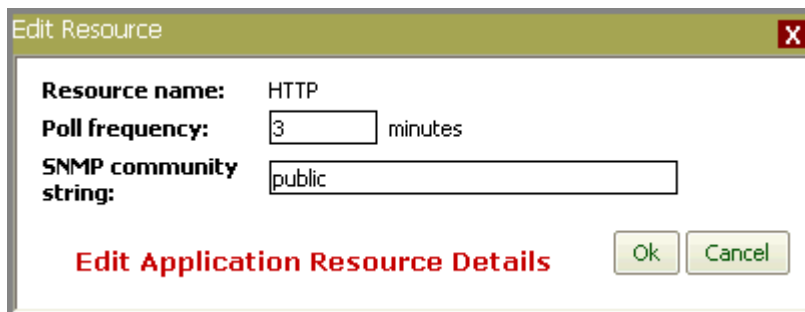
- 1 Click the system/application name dropdown, and select **Edit Resource**.
StatusTracker displays **Edit Resources** pop-up window.

Figure 77
Edit Resource-
System



A dialog box titled "Edit Resource" with a close button (X) in the top right corner. It contains the following fields: "Resource name:" with the value "MICKEY", "Display name:" with the value "MICKEY", "Device type:" with the value "Vista", "Poll frequency:" with a value of "3" and the unit "minutes", and "SNMP community string:" with the value "public". At the bottom, there is a red text label "Edit System Resource Details" and "Ok" and "Cancel" buttons.

Figure 78
Edit Resource-
Application



- 2 Make the appropriate changes in the respective fields, and then click the **Ok** button.

To view resource details

- 1 Click the system/application name dropdown, and select **Resource Details**. StatusTracker displays **Resources Details** pop-up window.

Figure 79
Resource details-
System

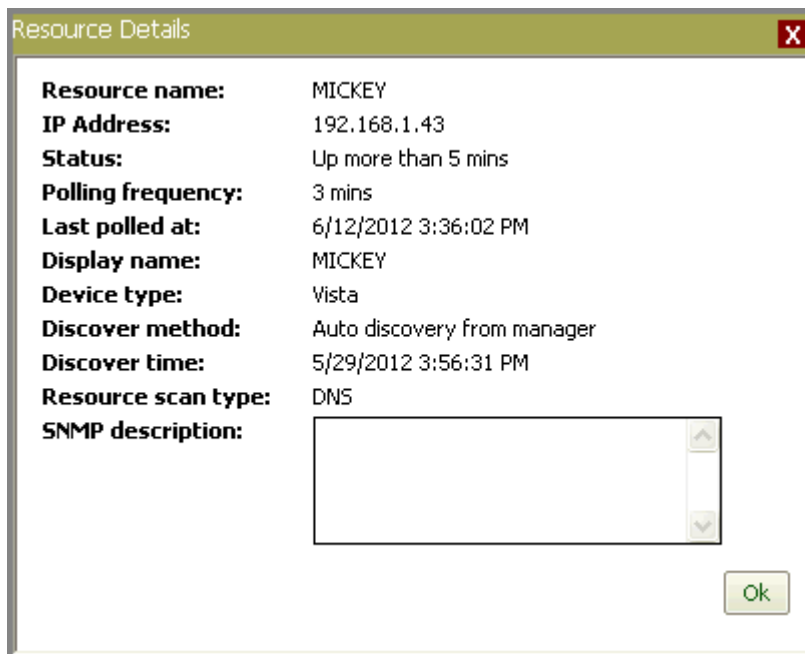
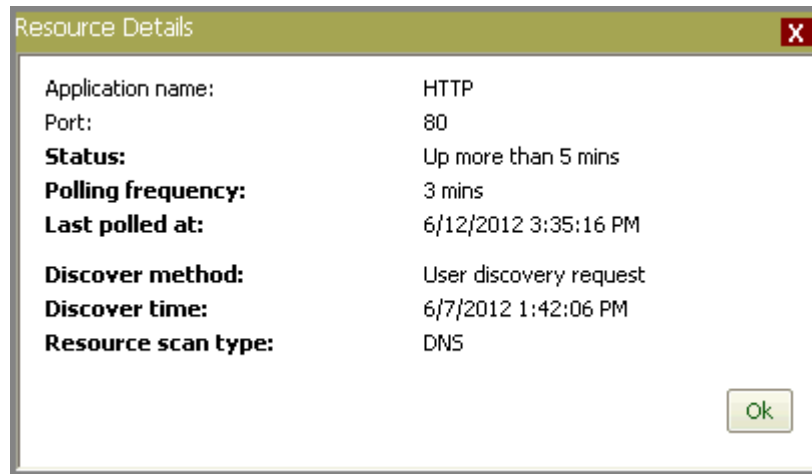


Figure 80
Resource details-
Application



- 2 Click the **Ok** button.

Polling Summary

Polling summary gives you the system/application status in a specified time period.

- 1 Click the system/application name dropdown, and select **Polling summary**. StatusTracker displays **Polling summary** dialog box.

Figure 81
Polling summary –
System

Polling Summary

Polling summary details for: **LUKE**

From: 6/11/2012 04 : 03 : 14 : PM

To: 6/12/2012 04 : 03 : 14 : PM

Export **Show**

Status	Polled date time
Maintenance	6/12/2012 2:59:17 PM
Initializing	6/12/2012 3:17:49 PM
Up	6/12/2012 3:17:51 PM

Close

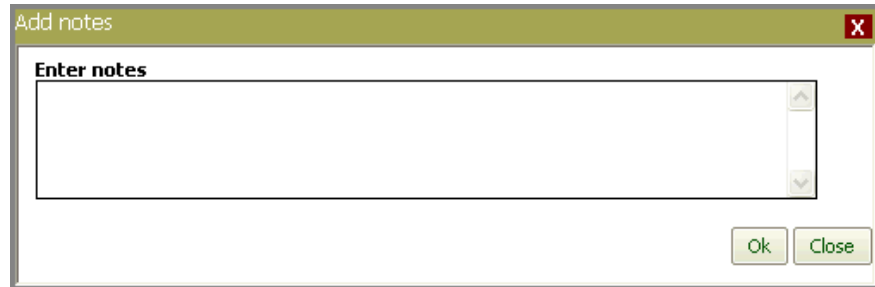
- 2 Select the duration of polling in **From** and **To** fields, and then click the **Show** button.
- 3 Click **Export**, if you wish to export the polling summary details in Excel sheet.
- 4 Click the **Close** button.

Add Notes

This option is provided to add extra information about the system or application. For example, it can be used to specify the reason for a system being put under maintenance.

- 1 Click the system/application name dropdown, and select **Add notes**.
StatusTracker displays **Add notes** pop-up window.

Figure 82
Add notes dialog box



- 2 Enter the system/application relevant details, and then click the **Ok** button.

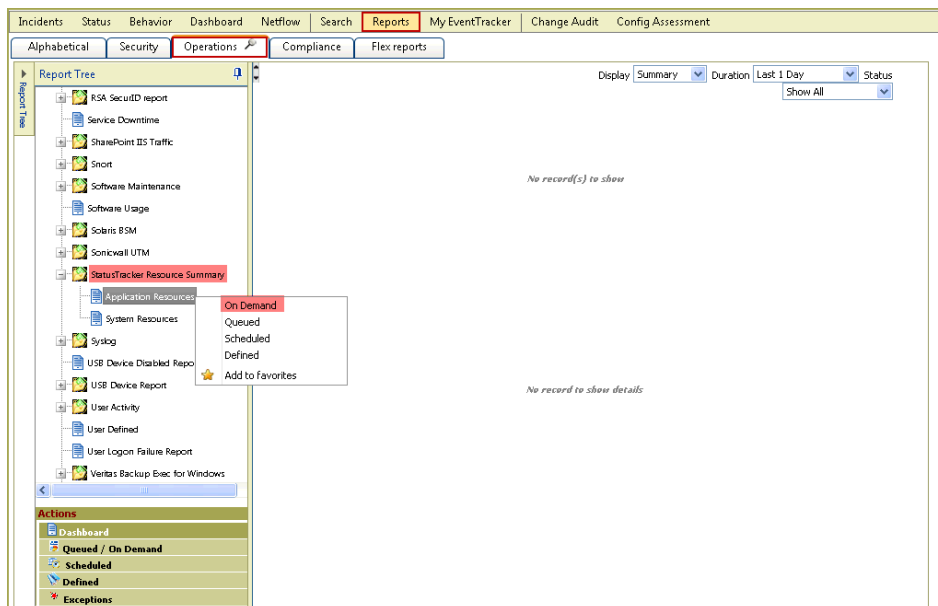
StatusTracker Reports

A StatusTracker report gives you the summary details of monitored system(s) or application(s) activities over a period of time. The results obtained from this report can be used to examine on how many systems/applications are added/deleted/modified, and the status of particular resource in a specific duration.

To generate StatusTracker Resource Summary

- 1 Click the **Reports** menu, and then click **Operations** tab.
- 2 In the **Report Tree** pane, scroll down to search for **StatusTracker Resource Summary**
- 3 Expand **StatusTracker Resource Summary**.

Figure 83
Report Tree-
StatusTracker
Resource Summary



- 4 Right click **Application Resources/System Resources**, and then select **On Demand**.
EventTracker displays **Reports Wizard**.
- 5 Click **Next >>**.
- 6 In the **Interval** pane, select the report duration in **Select interval/Select date range** field.
- 7 Check the '**Limit to time range**' option to limit the report time range to specified timings.
- 8 In **More options** pane, select the **Format option** and **Export type** from the respective dropdown.
- 9 Click **Next >>**.
- 10 If required, set the **Refine** and **Filter** criteria, and then click **Next >>**.
- 11 Enter appropriate Title, Header, Footer, and Description for the report, and then click **Next >>**.
- 12 Cross check the **Disk cost analysis for the report**, and then click **Next >>**.
- 13 Click **Generate report**.

To generate StatusTracker Resource Activities Report(s)

EventTracker also provides an option to summarize the group(s)/resource(s) activities in the StatusTracker over a given period. The activities can be change in resource status, addition/ removal/ modification of group/ resources etc. You can generate a report to see the changes happened in the StatusTracker group(s)/resource(s) within the specified time.

- 1 Click **Reports** menu, and then click **Operations** tab.
- 2 In the **Report Tree** pane, expand **EventTracker** category group.

Report	Contains
EventTracker: StatusTracker resource added	The details of system(s)/application(s) added in the group(s)/system(s) within the specified time.
EventTracker: StatusTracker resources deleted	The details of system(s)/application(s) deleted from the group(s) within the specified time.
EventTracker: StatusTracker resources down	The details of system(s)/application(s) whose status is 'Down' for a given time period.
EventTracker: StatusTracker resource group added	The details of the group(s), which are added in the StatusTracker in a given time period.
EventTracker: StatusTracker resource group deleted	The details of the group(s), which are deleted from the StatusTracker over a given period.
EventTracker: StatusTracker resource group modified	The details of the group(s), which are modified over a given period.
EventTracker: StatusTracker resource modified	The details of the resource(s), which are modified over a given period.
EventTracker: StatusTracker resource up	The details of system(s)/application(s) whose status is 'up' for a given time period.

- 3 Right click the required report, and then click the **On Demand**.
EventTracker displays 'Reports Wizard'.
- 4 Click **Next >>**.
- 5 Select system(s) or group(s) for the report, and then click **Next >>**.
- 6 In the **Interval** pane, select the report duration in **Select interval/Select date range** field.
- 7 Check the '**Limit to time range**' option to limit the report time range to specified timings.
- 8 In **More options** pane, select the **Format option**, **Export type**, **Chart type**, and **Sort by** options from the respective dropdown.
- 9 Click **Next >>**.
- 10 If required, set the **Refine** and **Filter** criteria, and then click **Next >>**.

- 11 Enter appropriate **Title, Header, Footer**, and **Description** for the report, and then click **Next >>**.
 - 12 Cross check the **Disk cost analysis for the report**, and then click **Next >>**.
 - 13 Select/enter required details, and then click **Next >>**.
 - 14 Click **Generate report**.
-

Chapter 4

Analyzing Enterprise Activities

In this chapter, you will learn how to:

- [Monitor Enterprise Activities](#)
- [Add Dashlets](#)
- [Analyze non-Admin User Activities](#)
- [Analyze Admin User Activities](#)
- [Analyze per System Activities](#)
- [Analyze IP Addresses by Traffic](#)
- [Analyze Processes by Occurrence](#)
- [Analyze Events by Occurrence](#)
- [Analyze Log on Failure Activity](#)
- [Analyze Runaway Process Activity](#)
- [Analyze Software Activity](#)
- [Analyze Network Activity](#)
- [Analyze Application Activity](#)
- [Monitor USB Activity](#)
- [Analyze USB Activity](#)
- [Configure Enterprise Activity Behavior Settings](#)
- [Manage Behavior Rules](#)
- [Add Behavior Rules](#)

Monitoring Enterprise Activities

Manually reviewing and analyzing enterprise wide event log data in order to identify patterns of suspicious behavior is a time consuming and tedious task, which leaves ample room for errors and missed conditions. In order to reliably get the right information, rules have to be defined for anomalous conditions - and these are only as good as the person writing the rules/performing the review. In addition, you have to know what you are looking for to write the rules.

EventTracker addresses this issue with its Enterprise Activity Monitor, a dashboard that automatically provides information about unusual behavior by:

- Continuously monitoring the event log stream
- Performing a combination of statistical and behavioral correlation
- Detecting both new activity and activities that significantly deviate from normal operations

Conditions detected include:

- Abnormally high or low admin and user activity
- Abnormally high or low system, process or IP activity
- First seen for IP addresses, admins, users, processes etc.
- Sudden changes in event volumes

Enterprise Activity Dashlets

EventTracker's enterprise activity dashboard is categorized into **Security** and **Operations**. The dashboard provides you dashlets with the predefined set of rules, and allows you to add **custom** dashlets created with your own rule set. It is left to your discretion to organize the dashlets as per your requirement. The security and operational activities of an enterprise are presented in graphical form in this dashboard. By Default, EventTracker displays the last 24-hour data.

The dashlets in the **Security** and **Operations** dashboard are not refreshed automatically. Click the refresh button to refresh the dashlet.

Behavior Dashboard	Security To monitor security related events	Admin Activity
		Application activity
		Event ID Activity
		IP address Activity
		Logon Failure Activity
		Network Activity
	Operations To monitor anomalies in system performance (CPU, disk, memory), service failures, network connections, printer usage etc.	Process Activity
		RunAway Process Activity
		Software Activity
		System Activity
		USB Activity
		User Activity
		User defined Activities

NOTE

For **Security** and **Operations** behavior, procedure to configure and customize dashlets, volume analysis, and reports generation are same.

Adding Behavior Dashlets

This option helps to add dashlets to view enterprise behavior.

To add dashlets

- 1 Log on to **EventTracker Enterprise**.
- 2 Click **Behavior** menu, and then click **Security/Operations** tab.

EventTracker displays the Behavior dashboard with default dashlets.

Figure 84
Security Dashboard

Behavior dashboard displays enterprise activities through default dashlets. Using **Customize** option the behavior dashlets can be added to the dashboard. Also new behavior dashlet can be added by creating custom **Behavior rule**.

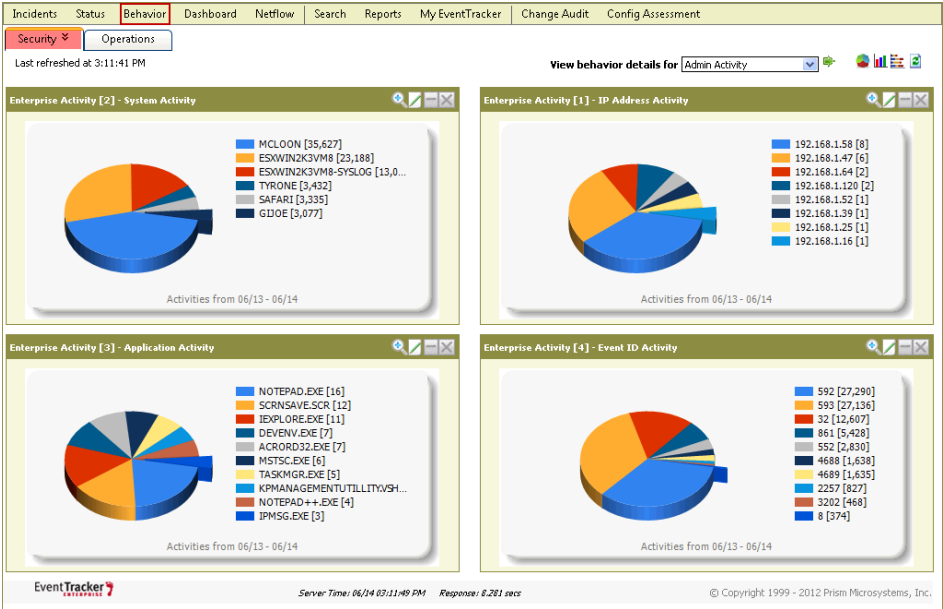
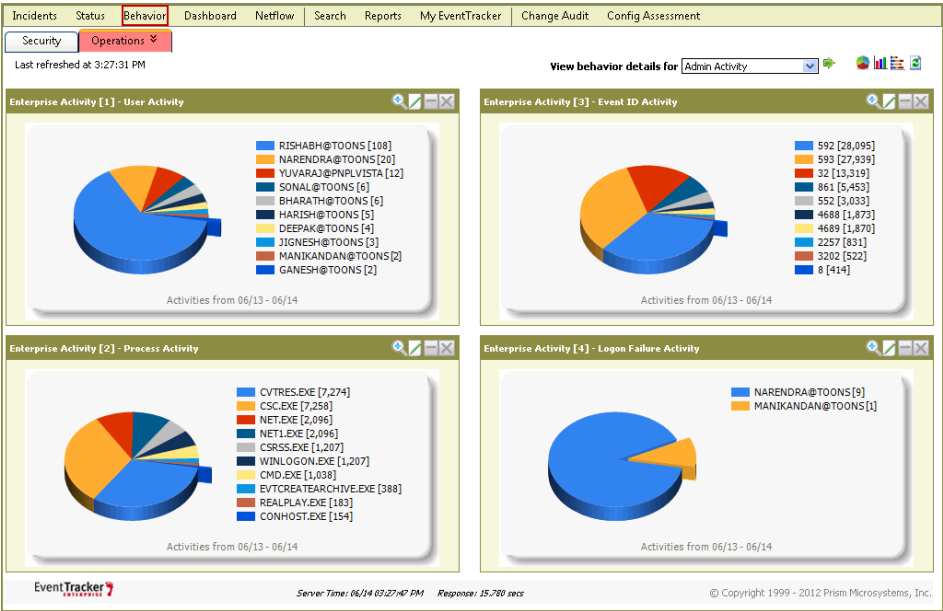
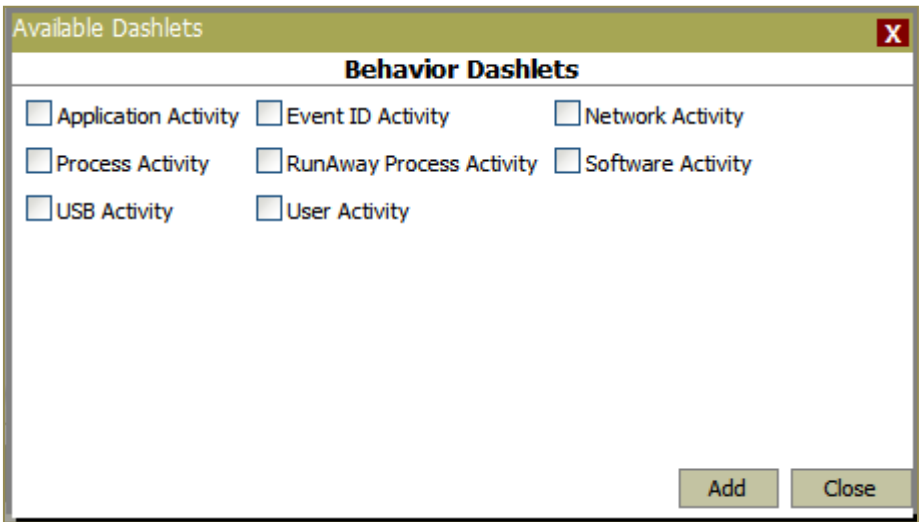


Figure 85
Operations
Dashboard



- 3 Click **Customize** on the shortcut menu.
EventTracker displays the **Available Dashlets** dialog box.

Figure 86
Adding Behavior
Dashlets

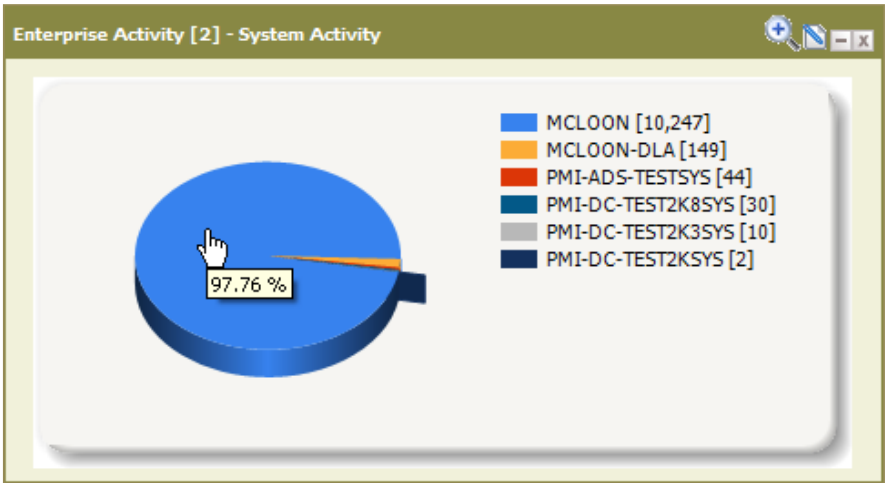


- 4 Check the required activity option, and then click **Add**.
EventTracker adds the selected dashlet to the dashboard.

Important To Know:

- Move the mouse pointer over a pie or the legend to view tooltip.

Figure 87
Tooltip



- Click a pie or legend.
- EventTracker moves you through Enterprise Activity Dashboard.

Analyzing User Activities

Non-admin User Activities

Following are the Event IDs considered for analyzing non-admin user activities.

Table 19

Non-Vista Systems
528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 551, 642, 644, 672, 675, 682, and 683
Vista Systems
4624, 4625, 4634, 4647, 4738, 4740, 4768, 4771, 4778, and 4779

Admin User Activities

Following are the Event IDs considered for analyzing admin user activities.

Table 20

Non-Vista Systems
608, 610, 611, 612, 618, 620, 621, 624, 626, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 641, 642, 643, 645, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 660, 661, 662, 663, 664, 665, 666, 668, 671, 685, 687, 689, 690, 691, 692, 693, 694, and 807
Vista Systems

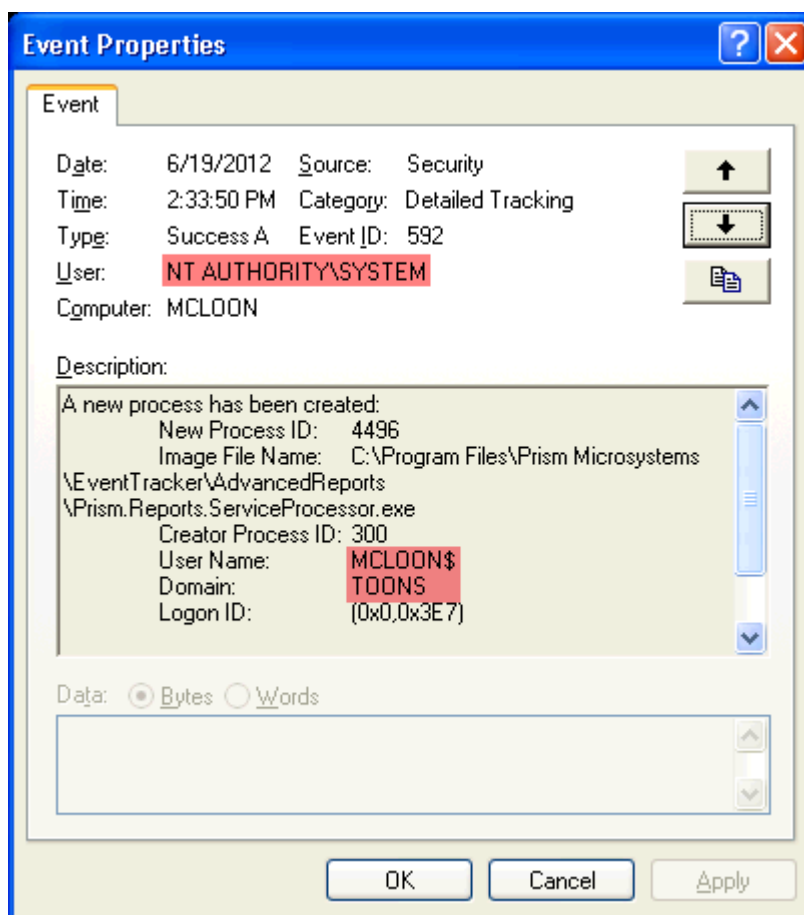
4670, 4706, 4707, 4714, 4715, 4716, 4720, 4722, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4739, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4764, 4765, 4766, 4767, 4781, 4782, 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4794, 4865, 4866, 4867, 4907, and 4912

User name and domain information is extracted from the **Event Properties**.

If the user name and domain information is not proper in the Event Properties, it is extracted from the **Event Description**. For example, if the user name is either 'LOCAL SERVICE' or 'ANONYMOUS LOGON' or 'N/A' or 'NETWORK SERVICE' or 'SYSTEM' or contains '\$' or contains 'USR' then the proper user name is extracted from the **Event Description**.

Also, if the domain name is either 'NT AUTHORITY' or 'N/A' then the proper domain name is extracted from the **Event Description**.

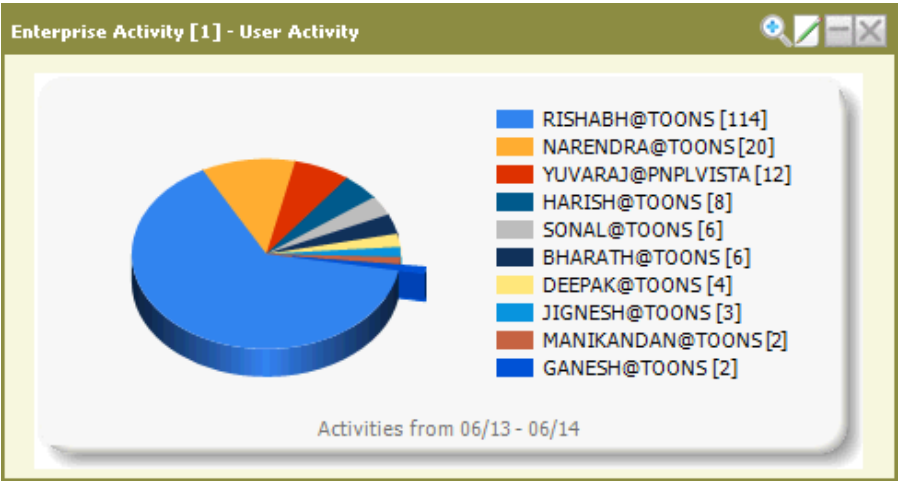
Figure 88
Event Properties
window



Analyze User Activities in Behavior Dashboard

- [Click the pie chart to view user activity details](#)

Figure 89
 Top 10 users by
 activity



EventTracker displays the 'Enterprise Activity Detail' page.

Figure 90
 Users by Activity
 details

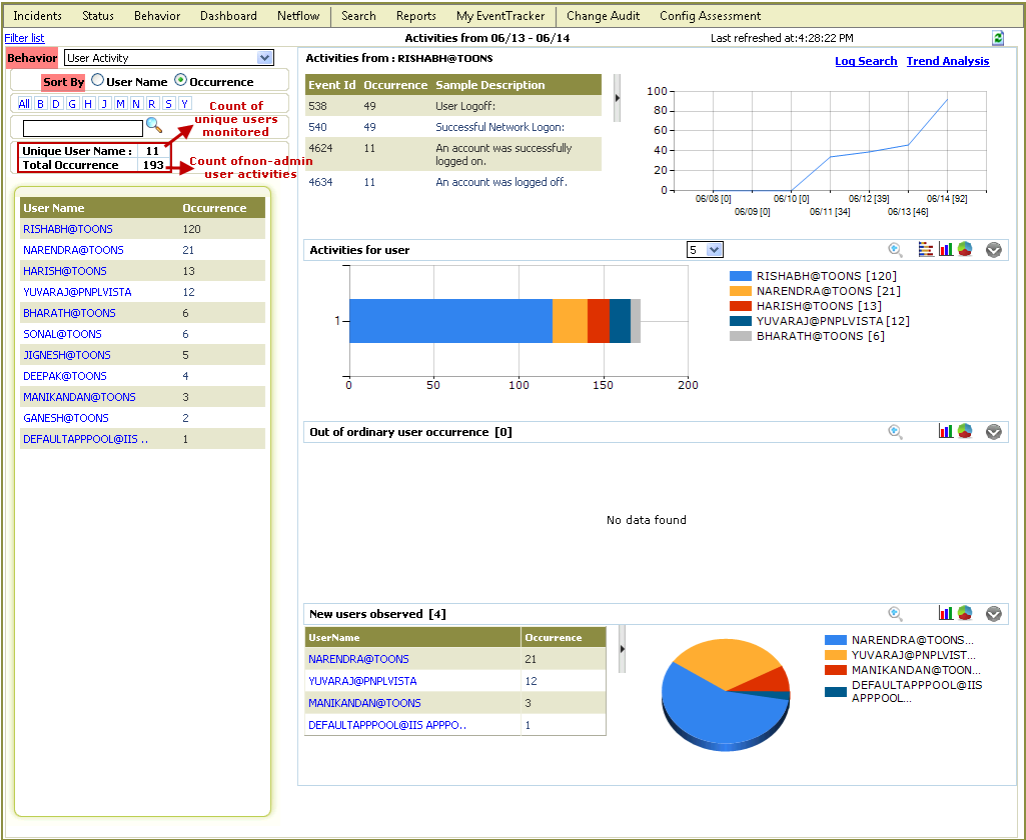











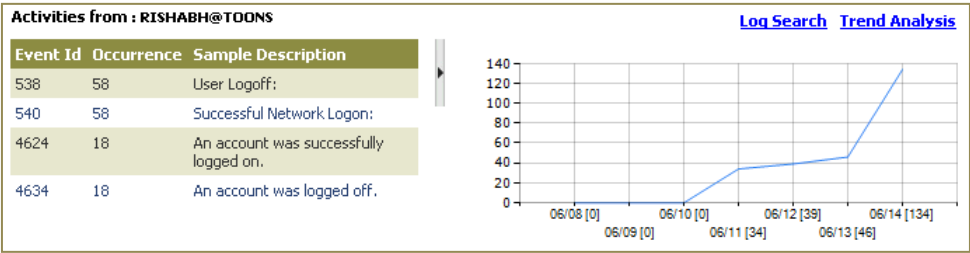
Table 21

Click	To
	Zoom a graph.
	Edit title of the graph.

	View Stacked Bar graph.
	View Bar graph.
	View Pie graph.
	Collapse a pane.
	Expand a pane.
	Collapse a pane.
	Expand a pane.
	Refresh the page with latest events
	Search the search phrase.

- **First pane** displays the activity details and the Weekly trend of activities

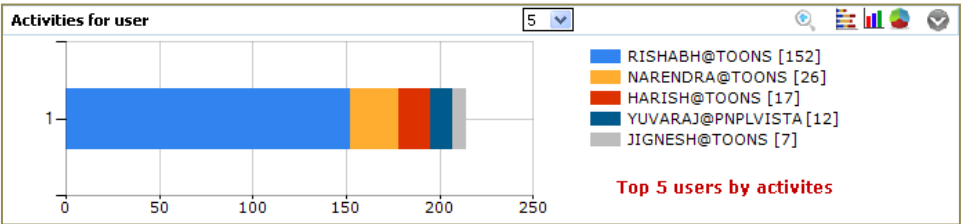
Figure 91
Event Details and
Weekly Trend



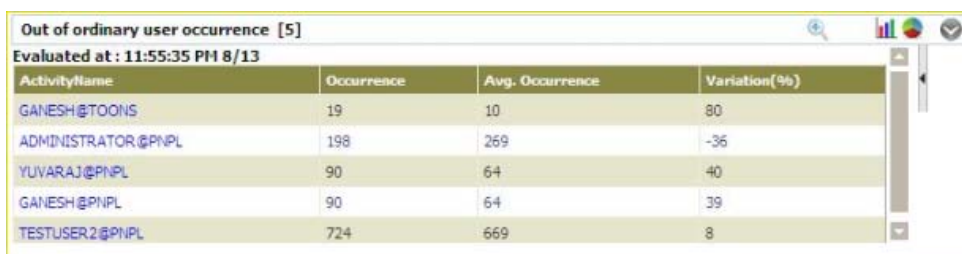
- **Second pane** displays top five users by activities

Options are provided to select number of users and chart type to view

Figure 92
Top user activities



- **Third pane** displays out of ordinary user activities, helps to monitor abnormal user activities

Figure 93
Out of ordinary user
activities


ActivityName	Occurrence	Avg. Occurrence	Variation(%)
GANESH@TOONS	19	10	80
ADMINISTRATOR@PNPL	198	269	-36
YUVARAJ@PNPL	90	64	40
GANESH@PNPL	90	64	39
TESTUSER2@PNPL	724	669	8

Table 22

Field	Description
Total Count	Total count of activities occurred during last 24 hours is displayed under this column.
Average Count	Average Count = Total count of activities / No. of days. Suppose the average count is taken on the 10 th day, total count of activities occurred in the past 9 days divided by 9 days gives you the Average Count.
Variation (%)	1. Positive Variation (when TotalCount - AvgCount = Positive) $\text{Variation\%} = ((\text{TotalCount} - \text{AvgCount}) / \text{AvgCount}) * 100$ 2. Negative Variation (when TotalCount - AvgCount = Negative) $\text{Variation\%} = ((\text{TotalCount} - \text{AvgCount}) / \text{TotalCount}) * 100$ If the positive variation is greater than the Behavior correlation threshold and the negative correlation is less than the negative of Behavior correlation threshold, then the activity is considered as out-of-ordinary activity.

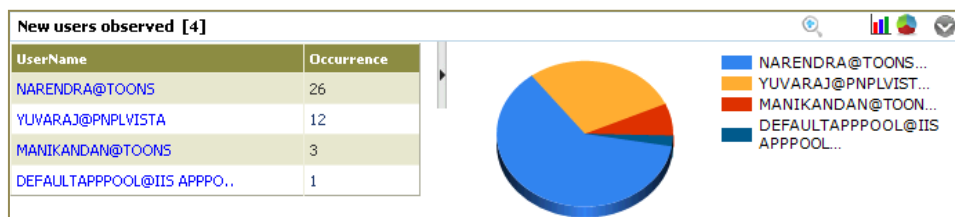
- Fourth pane displays new user activities**

Based on 'Behavior learning period", user is considered as 'New'.

If the activities after the behavior-learning period do not intersect with the activities during the behavior-learning period, then that user is considered as a 'New" user.

For example, the user activities occurred in the last 24 hours after the behavior-learning period is displayed in the '**New users observed**' pane. Similarly, if the **Generation interval** option is set as 'Last 2 days" or 'Last 3 days" respectively, then the user activities occurred in the last 48 hours and 72 hours after the 'Behavior learning period' is displayed in the '**New users observed**' pane.

Generation interval can be changed in 'Behavior Settings' page. Go to **Admin >> Behavior Settings** to change the enterprise activity interval.

Figure 94
New user activities

- **Left pane** displays the list of configured behavior rules

Click a hyperlink in the alphabetical list.

(OR)

Type the search phrase in the search field, and then click the search  icon

EventTracker displays the list of searched criteria.

Figure 95

All configured behavior rules will be shown in the **Behavior** dropdown list. On the selection of any rule from the dropdown, the sort by option, total occurrence and unique count of the rule will be displayed in the left pane.

Behavior User Activity

Sort By ☐ User Name ☒ Occurrence

All C D G H J K M N P R S

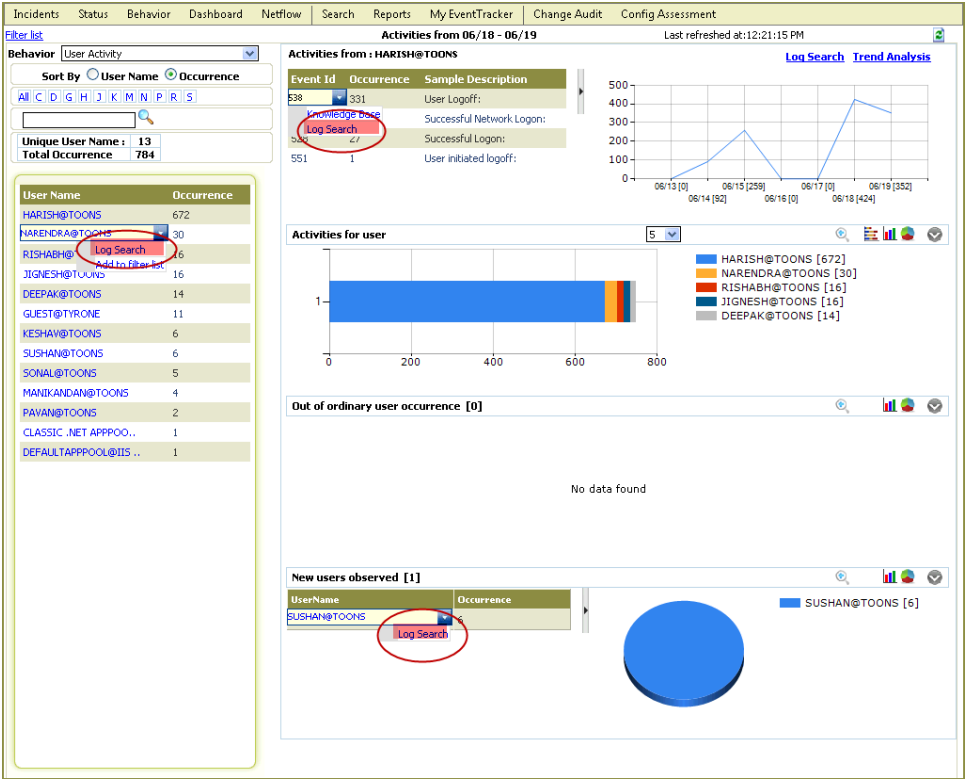
Unique User Name : 13

Total Occurrence 802

User Name	Occurrence
HARISH@TOONS	666
NARENDRA@TOONS	30
JIGNESH@TOONS	28
SUSHAN@TOONS	18
RISHABH@TOONS	16

- To do a **Log Search**, move the mouse pointer over a field in the first column on the left pane or in the first/ third/ fourth pane on the right side.
From the drop-down list, click **Log Search**.

Figure 96



EventTracker opens the Log Search browser with query results.

Figure 97
Log Search Window

Log search - Windows Internet Explorer

Refine Tags New search Analysis Export Total event count: 15

ID	Log Time	Event Properties	Event Description
1	6/23/2011 01:56:21 PM	Event ID: 538 Log Type: Security Event Type: Audit Success Category: 2 Source: Security Domain: TOONS Computer: MCLOON-DLA User: sonal	User Logoff: User Name: Sonal Domain: TOONS Logon ID: (0x0,0x2A367B8) Logon Type: 7
2	6/23/2011 01:56:21 PM	Event ID: 528 Log Type: Security Event Type: Audit Success Category: 2 Source: Security Domain: TOONS Computer: MCLOON-DLA User: sonal	Successful Logon: User Name: Sonal Domain: TOONS Logon ID: (0x0,0x2A367B8) Logon Type: 7 Logon Process: User32 Authentication Package: Negotiate Workstation Name: MCLOON Logon GUID: {9cd0a5b5-a9ff-f6da-f3d8-26ab6ea8562c}
3	6/23/2011 12:49:15 PM	Event ID: 538 Log Type: Security Event Type: Audit Success Category: 2 Source: Security Domain: TOONS Computer: MCLOON-DLA User: sonal	User Logoff: User Name: Sonal Domain: TOONS Logon ID: (0x0,0x1C2FA2E) Logon Type: 7
4	6/23/2011 12:49:15 PM	Event ID: 528 Log Type: Security Event Type: Audit Success Category: 2 Source: Security Domain: TOONS Computer: MCLOON-DLA User: sonal	Successful Logon: User Name: Sonal Domain: TOONS Logon ID: (0x0,0x1C2FA2E) Logon Type: 7 Logon Process: User32 Authentication Package: Negotiate Workstation Name: MCLOON

Search results for: User:SONAL AND domain:TOONS AND
id:528||529||530||531||532||533||534||535||536||537||538||539||540||551||642||644||672||675||682||683||4624||4625||4634||4647||4738||4740||4768||4771||4778||4779 , Timerange : 6/22/2011 2:27:59 PM - 6/23/2011 2:27:59 PM

Previous Next Stop New search Page: 1

- To view event details in the **EventTracker Knowledge Base**, move the mouse pointer over an event id under Event Id column in the first pane.
EventTracker displays the drop-down list.

Figure 98

Activities from : HARISH@TOONS

Event Id	Occurrence	Sample Description
538	356	User Logoff:
		Successful Network Logon:
528	27	Successful Logon:
551	1	User initiated logoff:

From the drop-down list, click **Knowledge Base**.
EventTracker displays the event details in the 'EventTracker Knowledge Base'.

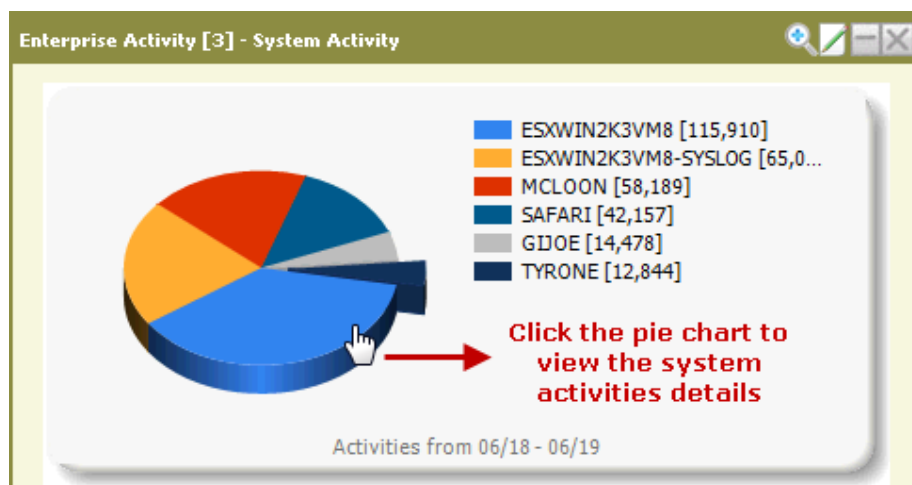
Analyzing Activities per System

This option helps you analyze activities occurred at systems. System name is extracted from the 'Event Properties'.

To analyze activities per system

- Click the **System Activity** pie chart to view the details of system activities in an enterprise.

Figure 99
System Activity



EventTracker displays the 'Enterprise Activity Detail' page.

Analyzing IP Addresses by Traffic

This option helps you analyze per IP trend of events.

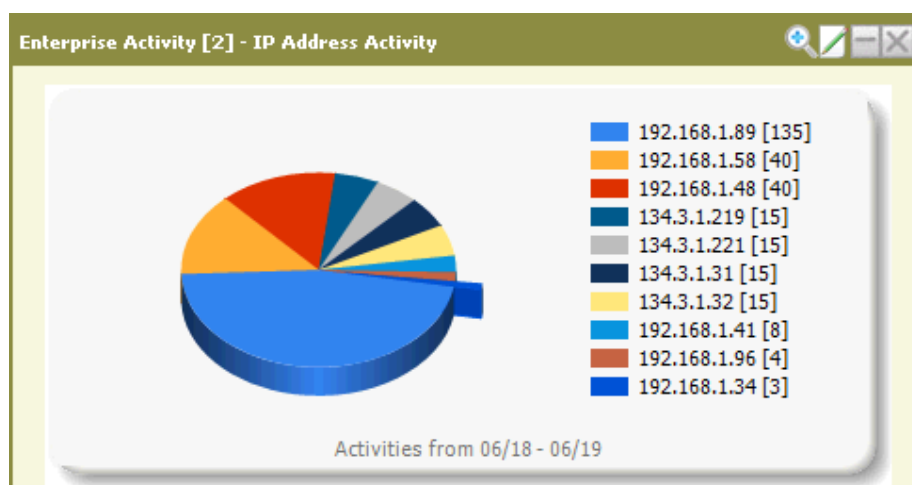
To analyze IP addresses by traffic

IP address is extracted from the **Event Description**. If the extracted string matches the loopback address '127.0.0.1' or local system IP '0.0.0.0' then it is filtered out. Otherwise, it is considered as a valid IP address.


- Click the **IP Address Activity** pie to view behavior details for IP address activities.

Figure 100
IP Address Activity

In case of **syslog** messages, the extracted string may resemble a valid IP address, which in reality is not. For instance, the version number of file xx.xx.xx.xx matches the pattern searched for but is not a valid IP.

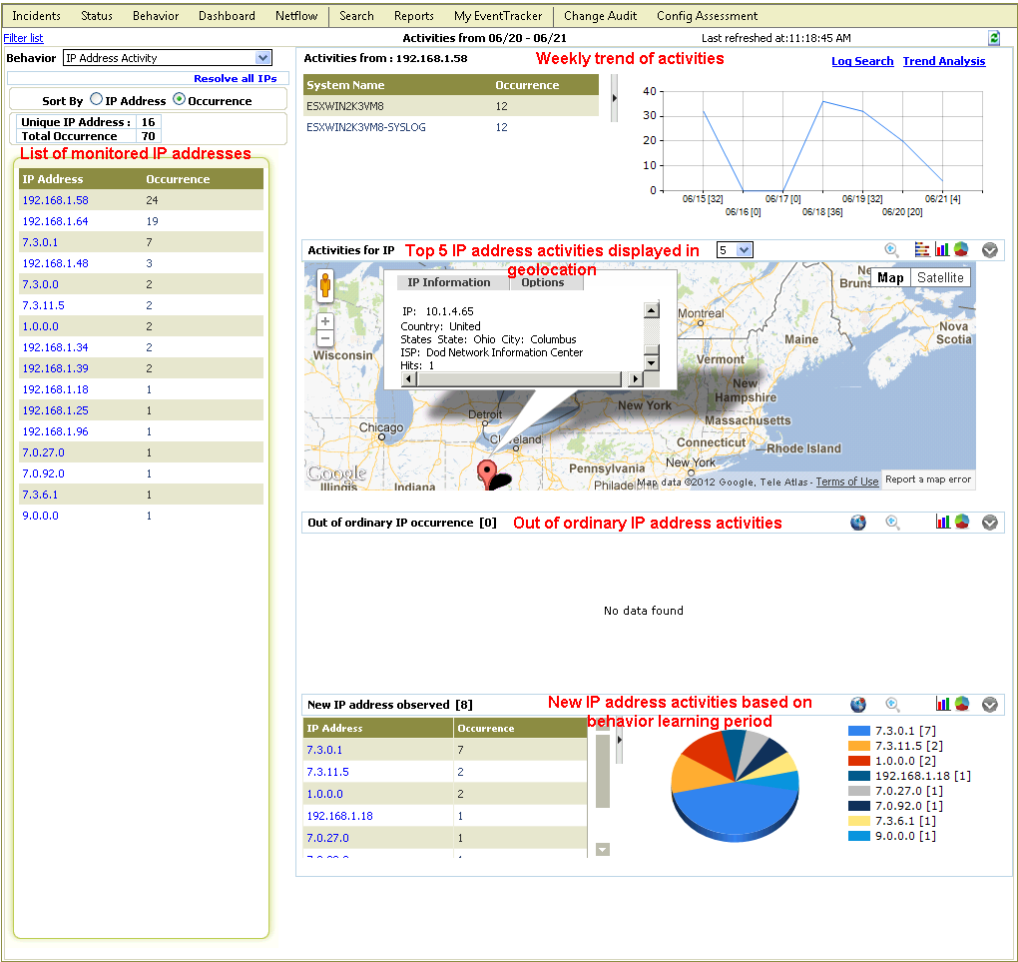


OR

From **View behavior details for** dropdown, select **IP Address Activity** option and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

Figure 101
IP address activities



'Out of ordinary IP occurrence' result is based on the criteria set in **Behavior Settings >> Threshold settings** pane or the configured **Behavior Rule**.

- To do a **Log Search**, move the mouse pointer over a row on the left pane or a row in the third and fourth panes.

From the drop-down list, click **Log Search**.

EventTracker opens the **Log Search** browser with query results.

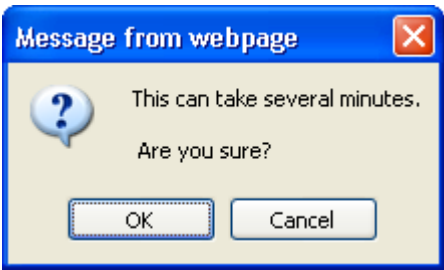
- The **Resolve all IPs** hyperlink is provided to get the DNS (Domain Name System) lookup for the respective IP addresses.

Click **Resolve all IPs** hyperlink.

EventTracker displays the confirmation message box.

Please wait while EventTracker resolves the IP

Figure 102
Confirmation
message box



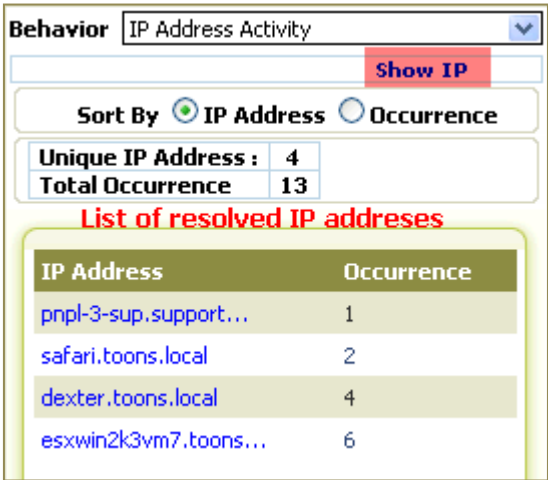
Click **OK** to proceed further.

EventTracker starts resolving the IP addresses. Use the **Stop** hyperlink to abort the action.

Once resolved, the DNS names will be reflected in the list.

Figure 103
Resolved IP
addresses

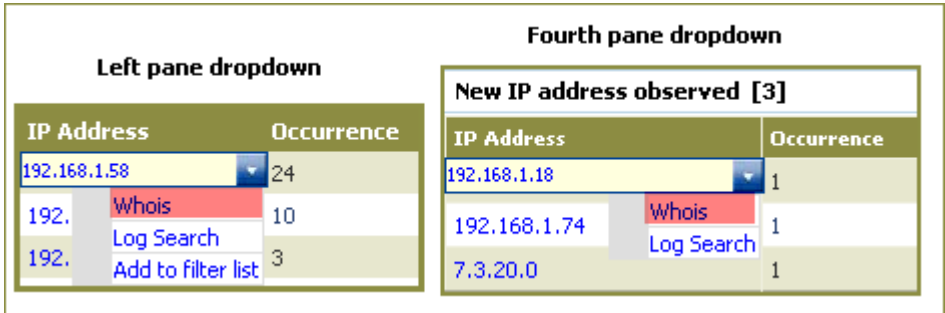
Use the **Show IP** hyperlink to resolve hostnames.



- **Whois** option is provided to resolve **WAN IP** addresses and to know the owner details.

Click the **IP address** dropdown in the left pane/ third pane/ fourth pane, and then select **Whois**.

Figure 104
Options to resolve
WAN IP addresses



EventTracker moves you through the '**DomainTools**' Web site.

Figure 105
Whois Lookup

DomainTools

Open a FREE Account | Log in | Help

Enter search term... Whois Search Search

HOMERESEARCHMONITORBUY DOMAINSLEARNOPEN AN ACCOUNT

IP Information for 192.168.1.125

IP Location:Private Ip Address Lan

ASN:AS32277

IP Address:192.168.1.125 W R P D T

Reverse IP:4 websites use this address. (examples: biz2go.info newagewow.com suolove.com youcanchina.com)

NetRange:192.168.0.0 - 192.168.255.255
CIDR:192.168.0.0/16
OriginAS:
NetName:PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:NET-192-168-0-0-1
Parent:NET-192-0-0-0
NetType:IANA Special Use
Comment:This block is used as private address space.
Comment:Traffic from these addresses does not come from IANA.
Comment:IANA has simply reserved these numbers in its database
Comment:and does not use or operate them. We are not the source
Comment:of activity you may see on logs or in e-mail records.
Comment>Please refer to http://www.iana.org/abuse/
Comment:
Comment:Addresses from this block can be used by
Comment:anyone without any need to coordinate with
Comment:IANA or an Internet registry. Addresses from
Comment:this block are used in multiple, separately
Comment:operated networks.
Comment:
Comment:This block was assigned by the IETF in the
Comment:Best Current Practice document, RFC 1918
Comment:which can be found at:
Comment:
Comment:http://www.rfc-editor.org/rfc/rfc1918.txt
RegDate:1994-03-15
Updated:2011-04-12
Ref:http://whois.arin.net/rest/net/NET-192-168-0-0-1

OrgName:Internet Assigned Numbers Authority
OrgId:IANA
Address:4676 Admiralty Way, Suite 330
City:Marina del Rey
StateProv:CA
PostalCode:90292-6695
Country:US
RegDate:
Updated:2004-02-24
Ref:http://whois.arin.net/rest/org/IANA

OrgTechHandle:IANA-IP-ARIN
OrgTechName:Internet Corporation for Assigned Names and Number
OrgTechPhone:+1-310-301-5820
OrgTechEmail:abuse@iana.org
OrgTechRef:http://whois.arin.net/rest/poc/IANA-IP-ARIN

OrgAbuseHandle:IANA-IP-ARIN
OrgAbuseName:Internet Corporation for Assigned Names and Number
OrgAbusePhone:+1-310-301-5820
OrgAbuseEmail:abuse@iana.org
OrgAbuseRef:http://whois.arin.net/rest/poc/IANA-IP-ARIN

Memberships | Developer API | About Us | Blog | Desktop Tools | Terms of Service | Privacy | Support | Careers | Contact Us | Site Map

© 2011 DomainTools, LLC All rights reserved.

Analyzing Processes by Occurrence

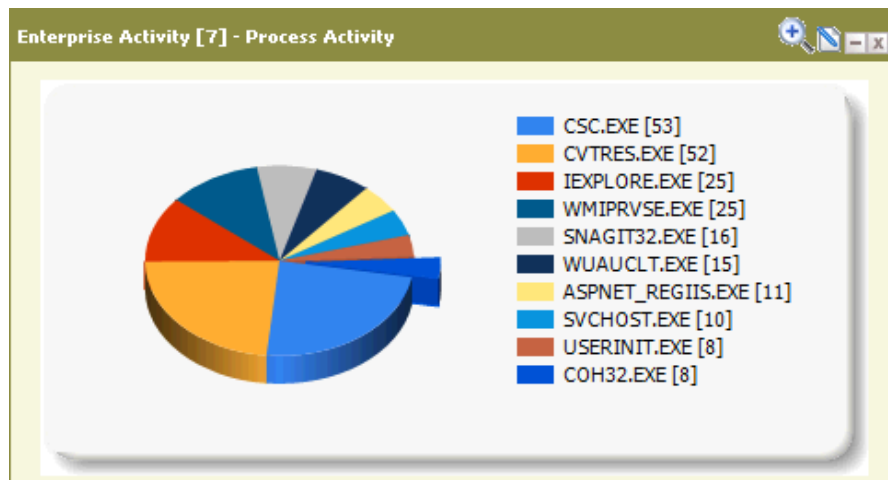
This option helps you analyze per user per system process utilization.

To analyze processes by occurrence


Event IDs **592 (non-Vista systems)** and **4688 (Vista systems)** are considered for process activity. Information like process name, process id, user name, domain name, and computer name are extracted from the 'Event Description'.

- Click the **Process Activity** pie chart to view process utilization activities details.

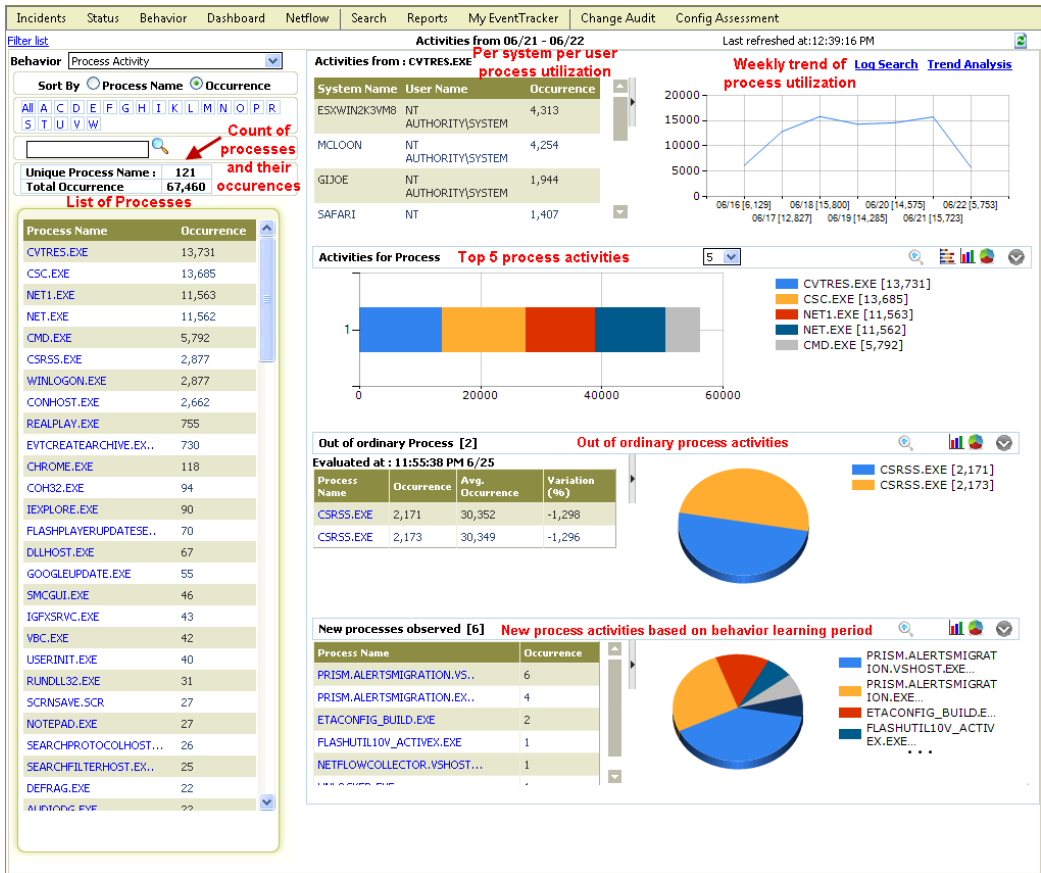
Figure 106
Process Activity



OR

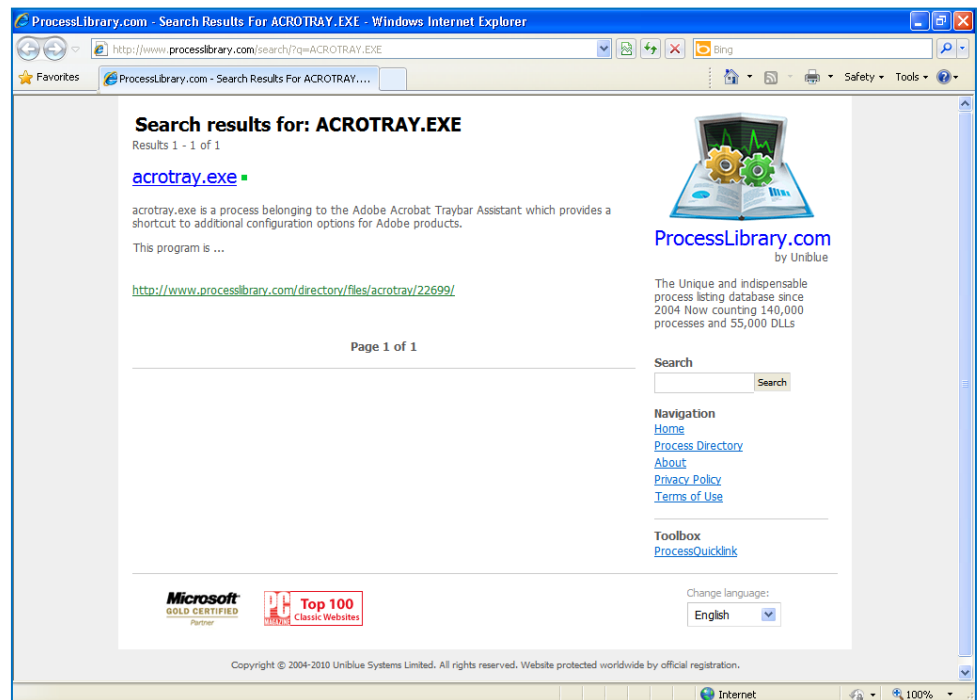
From **View behavior details for** dropdown, select **Process Activity** option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.



- To do a **Log Search**, move the mouse pointer over a row on the left pane or a row in the first/ third/ fourth pane.
From the drop-down list, click **Log Search**.
EventTracker opens the **Log Search** browser with query results.
- To find out more information on a process in 'ProcessLibrary' Web site, click the process name dropdown on the left/ third/ fourth pane, and then select '**What is this?**'
EventTracker moves you through the 'ProcessLibrary' Web site.

Figure 107
Process Library



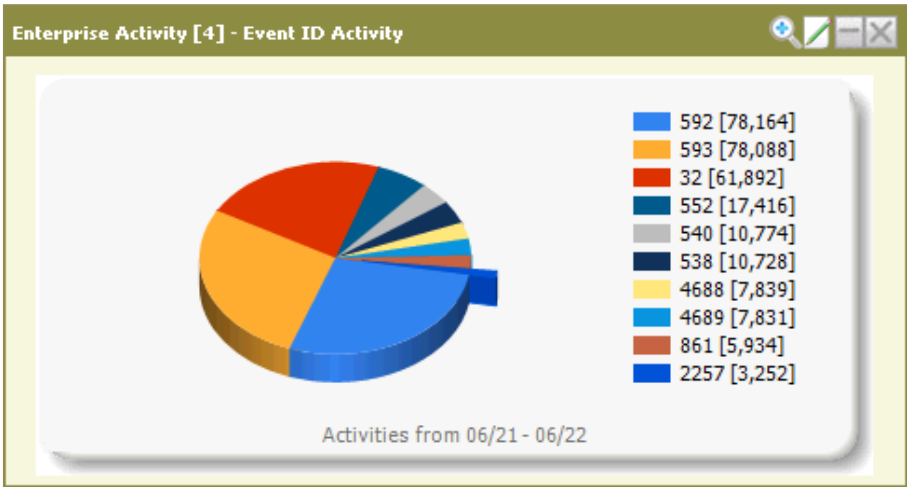
Analyzing Events by Occurrences

This option helps you analyze events by occurrence.


To analyze events by occurrences

- Click the **Event ID Activity** pie chart to view per event activity details.

Figure 108
Event ID Activity



OR

From **View behavior details for** dropdown, select **Event ID Activity** option, and then click the  icon.

EventTracker displays the 'Enterprise Activity Detail' page.

Analyzing Log on Failure Activity

This option helps you analyze log on failure events.

To analyze log on failure events

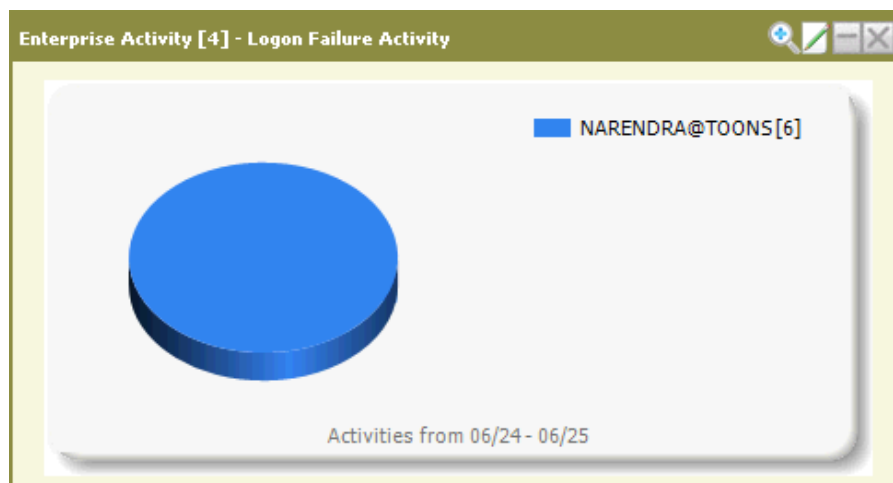
The Event IDs considered under this activity are:

Event ID
529, 530, 531, 532, 533, 534, 535, 536, 537, 539, 545, 675, 676, 4625, 4771 and 4772


Whenever these events are received, username is extracted and its count is maintained.

- Click the **Logon Failure Activity** pie chart to view per log on failure activity details.

Figure 109
Logon Failure
Activity



OR

From **View behavior details for** dropdown, select **Logon Failure Activity** option, and then click the  icon.

EventTracker displays the 'Enterprise Activity Detail' page.

Analyzing RunAway Process Activity

This option helps you analyze runaway processes.

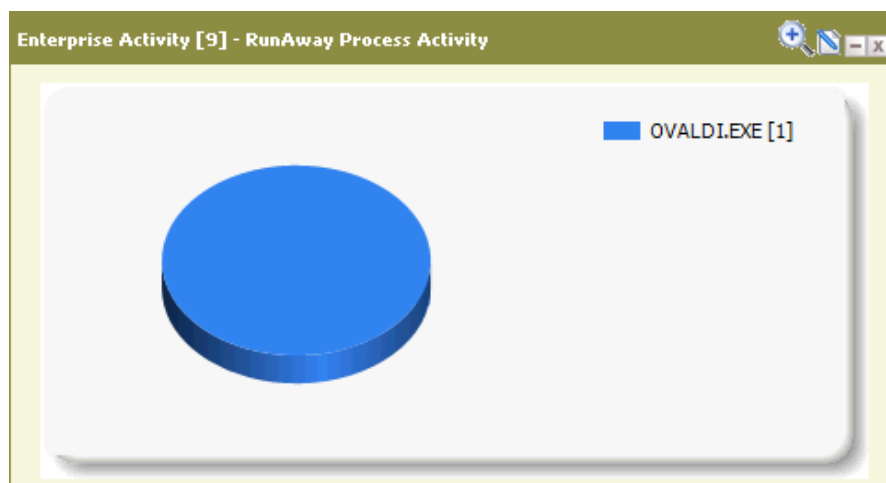
To analyze runaway processes

Event IDs considered under this activity are **3217** and **3218**.


Whenever **3217** and **3218** events are received, process and system names are extracted and its count is maintained. Left pane would list the process names and right pane would list two counts for that process, one for high memory usage and one for high CPU usage.

- Click the **RunAway process Activity** pie chart to view per runaway process activity details.

Figure 110
RunAway Process
Activity



OR

From **View behavior details for** dropdown, select **RunAway process Activity** option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

Analyzing Software Activity

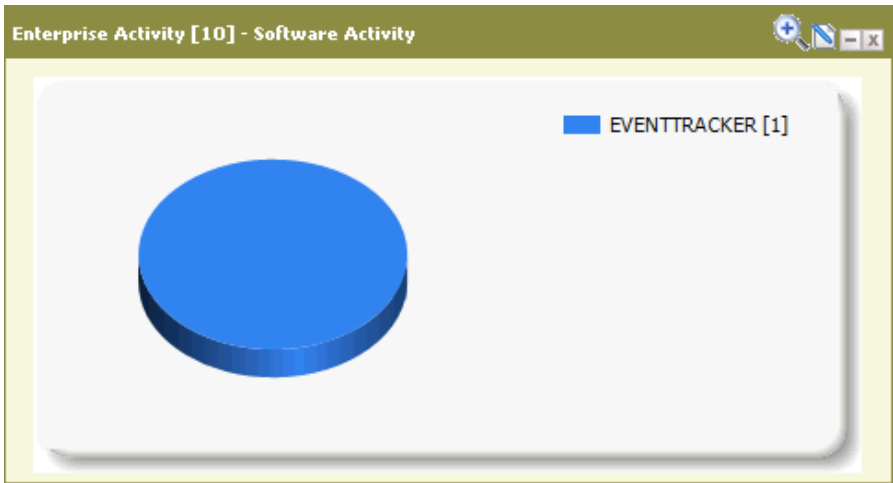
This option helps you analyze software activity.

To analyze software activity


Event ID considered under this activity is **3208**. Whenever 3208 event is received, software name and system name are extracted from the event, and its count is maintained. Left pane would list the softwares and right pane would give breakup for each software by system name and count.

- Click the **Software Activity** pie chart to view the software activity details per system.

Figure 111
Software Activity



OR

From **View behavior details for** dropdown, select **Software Activity** option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

Analyzing Network Activity

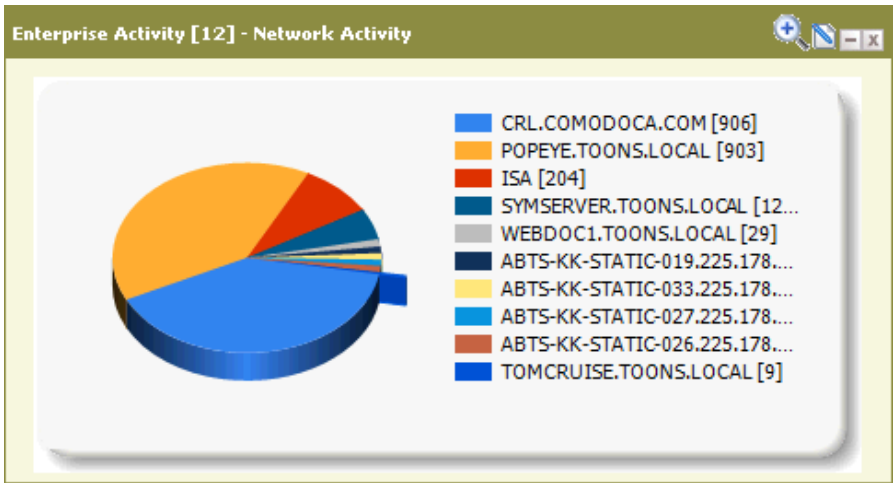
This option helps you analyze network activities.

To analyze Network activity


Event ID considered under this activity is **3223**. Whenever 3223 event is received, remote IP address and remote port information is extracted from the event, and its count is maintained.

- Click the **Network Activity** pie chart to view the activity details of devices like printers, routers over the respective network.

Figure 112
Network Activity



OR

From **View behavior details for** dropdown, select **Network Activity** option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

Analyzing Application Activity

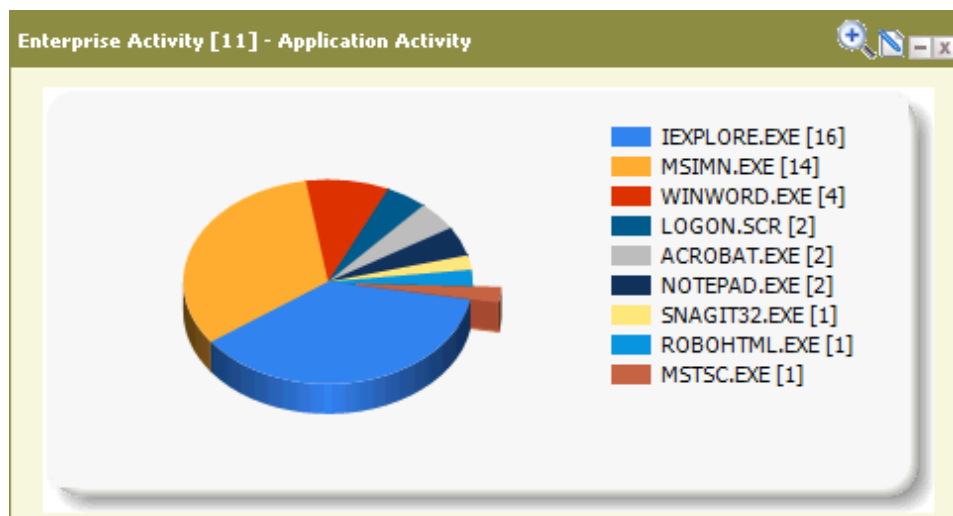
This option helps you analyze Application activity.

To analyze Application activity


Event ID considered under this activity is **3221**. Whenever 3221 event is received, application and system names are extracted from the event, and its count is maintained. Left pane would list the applications and right pane would give breakup for each application by system name and count.

- Click the **Application Activity** pie chart to view application activity details per system.

Figure 113
Application Activity



OR

From **View behavior details for** dropdown, select **Application Activity** option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

Analyzing USB Activity

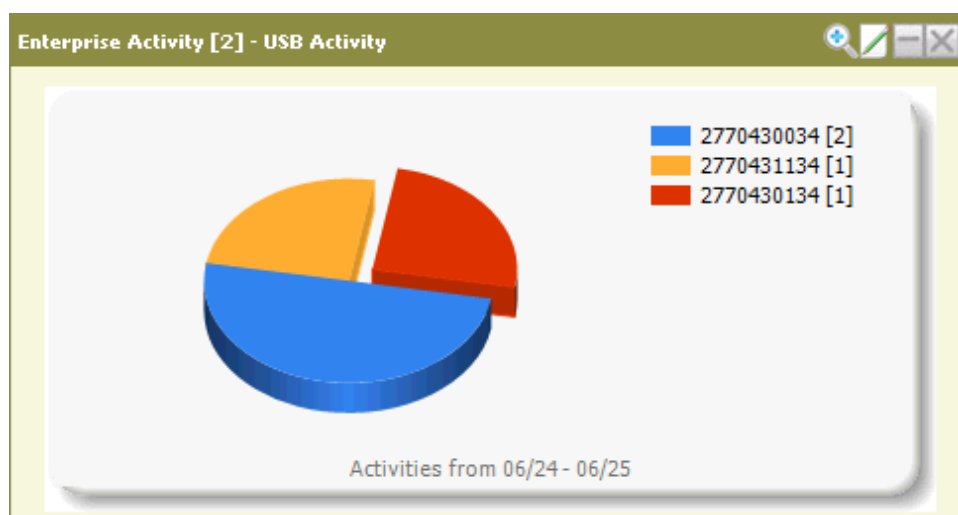
This option helps you analyze USB activity.

To analyze USB activity


Event ID considered under this activity is **3221**. Whenever 3221 event is received, application and system names are extracted from the event, and its count is maintained. Left pane would list the applications and right pane would give breakup for each application by system name and count.

- Click the **USB Activity** pie chart to view USB activity details per system.

Figure 114
USB Activity



OR

From **View behavior details for** dropdown, select **USB Activity** option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

Monitoring USB Activity

EventTracker provides advanced monitoring and analysis of the usage of these devices including:

- Tracking Insert/Removal
- Recording all activity (file writes to)
- Disabling according to predefined policy

With EventTracker, you can, for example:

- Set a policy that permits only certain devices to be used on servers
- Continuously monitor all USB usage on workstations
- Alert in real-time on the insertion of devices
- Block a specific device, if necessary
- Record all files that a user is writing to the USB

Included in the EventTracker Reports Engine are pre-packaged reports that can display all USB activity, including:

- Who the user was,
- What type of device was used
- What files were copied to the device

A complete inventory is captured that can be used for real-time analysis as well as a powerful forensic tool.

For more information, refer the [Monitoring System Health](#) section.


Configuring Behavior Filters

This option helps to configure behavior filters.

To configure behavior filters

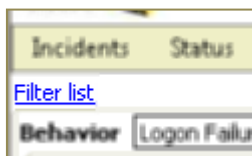
- 1 Click a pie chart to view **Enterprise Activity** page.

OR

From **View behavior details for** dropdown, select an activity option, and then click the  icon.

EventTracker displays the '**Enterprise Activity Detail**' page.

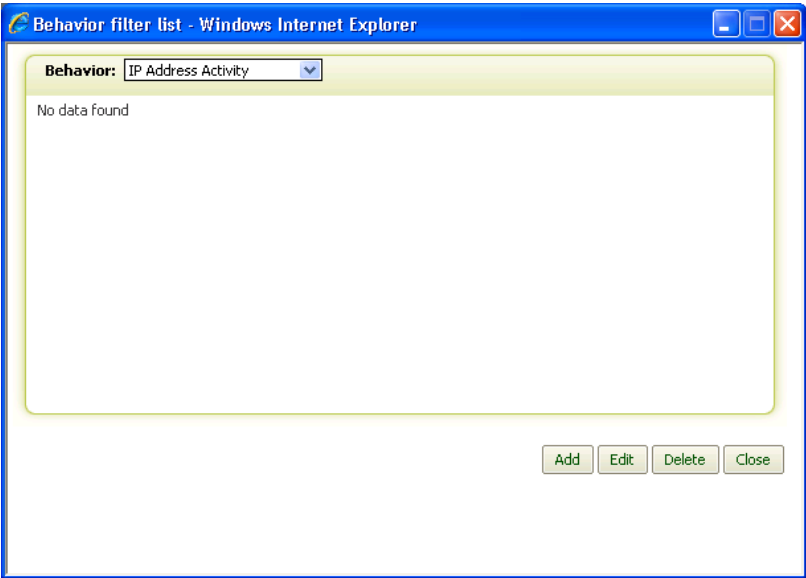
- 2 Click the **Filter list** hyperlink at the upper-left corner.



EventTracker displays the **Behavior filter list** dialog box.

Figure 115

Figure 116
Behavior Filter list



- 3 From the **Behavior** dropdown, select a behavior where you wish to apply the filter. Example: IP Address Activity
- 4 Click **Add**.

Figure 117
Behavior Filter list

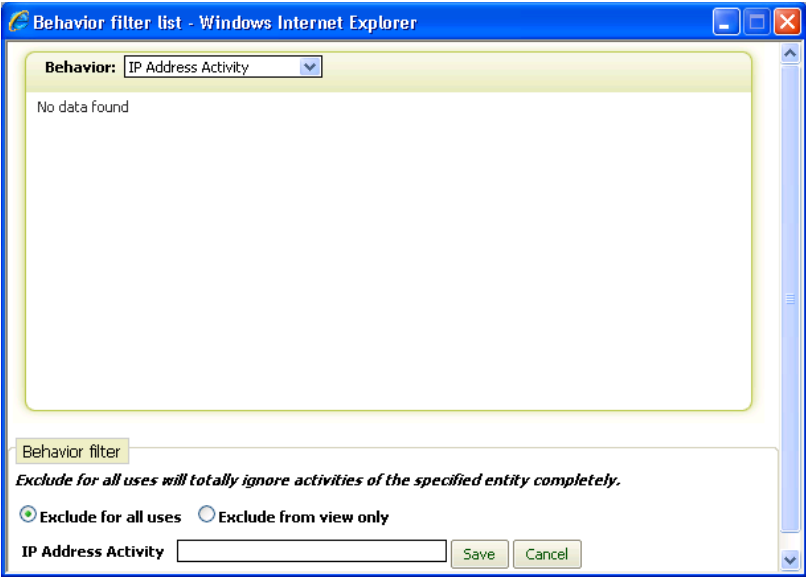


Table 23

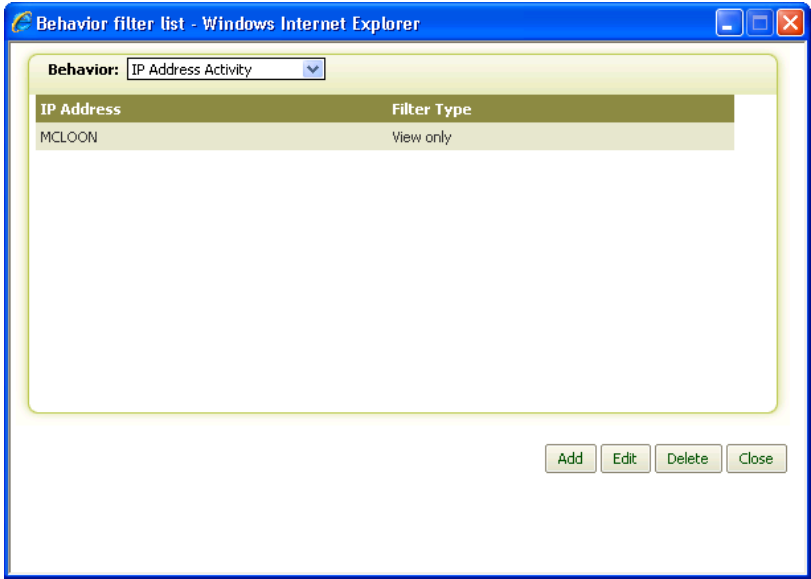
Field	Description
Exclude for all users	Totally ignore activities of the specified entity completely.

Exclude from view only	Hide the matches from the Enterprise Activity Dashboard.
<Behavior> Activity	Type the entity that you wish to filter.

- 5 Select an appropriate exclude option.
- 6 Type the entity that you wish to filter in the <Behavior> activity field.
- 7 Click **Save**.

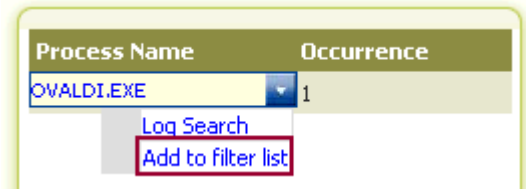
EventTracker adds the newly added filter to the filters list.

Figure 118
Behavior Filter list



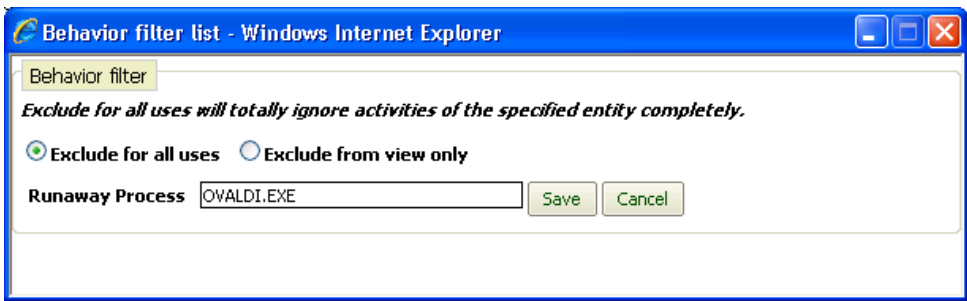
(OR)

In the **Enterprise Activity** page, click the dropdown of an entity on the left pane, and then click **Add to filter list**.



EventTracker displays the **Behavior filter list** dialog box.

Figure 119
Behavior Filter list



Click **Save**.

Once the filter is set, EventTracker refreshes and displays the 'Enterprise Activity Detail' page in sync with the filters set.

Volume Analysis

Volume analysis helps to analyze enterprise activity log volume.

This option provides a summary of total enterprise activities with respect to **Security** or **Operation**, which provides the distinct count of the activities and the total count of its occurrences.

To analyze enterprise activity log volume

- 1 In the **Behavior** menu, click **Security** or **Operations** dropdown, and then select **Volume Analysis**.



EventTracker displays the **Volume Analysis** dialog box.

Figure 120
Security and
Operations
dropdown

Figure 121
Enterprise log
Volume Analysis

Volume Analysis		
Behavior▲	Unique	Total Count
Admin Activity	0	0
Application Activity	43	238
Event ID Activity	111	365,204
IP Address Activity	18	164
Logon Failure Activity	7	135
Network Activity	0	0
Process Activity	169	73,703
RunAway Process Activity	1	1
Software Activity	0	0
System Activity	21	365,204
USB Activity	3	4
User Activity	22	1,230

Table 24

Field	Description
Behavior	List of activities. Click Behavior to sort the list in ascending or descending order.
Unique	Count of unique activities.
Total Count	Total count of occurrences with respect to unique activities.

- 2 Click an activity hyperlink to search the selected activity within a specified time range.

Figure 122
Enterprise log
Volume Analysis

Volume Analysis

Application Activity

☐ Display all records ☒ Display only top 10

Select Time Range

From: 6/25/2012 11 : 37 : 23 : AM

[mm/dd/yyyy] [hh:mm:ss]

To: 6/26/2012 11 : 37 : 23 : AM

Generate Close

- 3 Select **Application Activity** option, set appropriate **time range**, and then click **Generate**.

EventTracker displays the consolidated list of activities.

Figure 123
Enterprise log
Volume Analysis

Volume Analysis - Windows Internet Explorer

Behavior volume analysis

From date : 6/25/2012 11:37:23 AM To date : 6/26/2012 11:37:23 AM

Detailed Behavior report per Application

Unique Applications : 10 Total Count : 157

Application Name	Occurrence
IEXPLORE.EXE	71
NOTEPAD.EXE	24
CMD.EXE	21
FIREFOX.EXE	8
EXPLORER.EXE	6
MSTSC.EXE	6
SCRNSAVE.SCR	6
DEVENV.EXE	5
MMC.EXE	5
MSACCESS.EXE	5

- 4 Click the **Print** hyperlink to print the report.

Enterprise Activity Behavior Settings

This option helps you configure Enterprise Activity monitoring parameters.

To configure Enterprise Activity Behavior Settings

- Click **Admin** hyperlink, click **Control Panel** tab, and then click **Behavior Settings** hyperlink.

(OR)

- Click the **Admin** dropdown, and then select **Behavior Settings**.

EventTracker displays the Behavior Settings page.

Figure 124
Enterprise Activity
Behavior Settings

Behavior Settings

User Activity

☒ Monitor enterprise activity

Event threshold

Event 3269 is generated when the total count of Admin, non-admin user activities exceed the threshold. Set the maximum event threshold per user that is pertinent to your environment.

Event threshold(number of activities) per user: 2500

Purge Frequency

Deletes the activity data, which is older than the configured number of days.

☒ Purge user data older than 15 days

Threshold settings

Minimum count: 1000

☒ Variation: 200 %

☒ Behavior learning period: 7 days

Top Activities

Top activities displayed: 200

Generation Interval

Select the enterprise activity interval: Last 1 Day

☒ Enable DNS lookup for IP addresses: http://whois.domaintools.com/IP-ADDRESS

☒ Enable Process lookup for applications: http://www.processlibrary.com/search/?q=


Geolocation Setting

☒ Enable geolocation using API key: [API Key]

Ok Cancel

Table 25

Field	Description
User Activity	
Monitor enterprise activity	This parameter is used for backward compatibility. Any time any user crosses 2500 (default) activities - EventTracker will generate an event. This is only for user and admin activity (IP, process, alerts and event-ids are excluded)
Event threshold	

Event Threshold [number of activities] per user	Event 3269 is generated when the total count of Admin, non-admin user activities exceed the threshold. Set the maximum event threshold per user that is pertinent to your environment.
Purge Frequency	
Purge user data older than	EventTracker purges the enterprise activity data older than the configured number of days.
Threshold settings	
Minimum Count	This is a preliminary check for out-of-ordinary activity. The behavior correlation is performed for a particular activity only if it exceeds the threshold.
Variation	This is a preliminary check for out-of-ordinary activity. Behavior correlation is performed for a particular activity, only if this threshold is crossed.
Behavior learning period	This parameter is used for behavior correlation as well as for identifying new object. Based on the statistics prepared on the data collected during this period, an activity is declared whether it is new or out-of-ordinary activity.
Top activities	
Top activities displayed	Only the selected number of activities will be displayed on the left hand side pane of the 'Enterprise Activity Details' page.
Generation Interval	
Select the enterprise activity interval	Enterprise activities are displayed for the selected number of days.
Enable DNS lookup for IP addresses	Select this checkbox to resolve IP addresses.
Enable Process lookup for applications	Select this checkbox to know more about the processes.
Geolocation Setting	
Geolocation Setting	Enterprise Activity Details page displays IP addresses in geolocation map. Provide geolocation API key to activate geolocation. Click  icon to know how to get API key for geolocation.

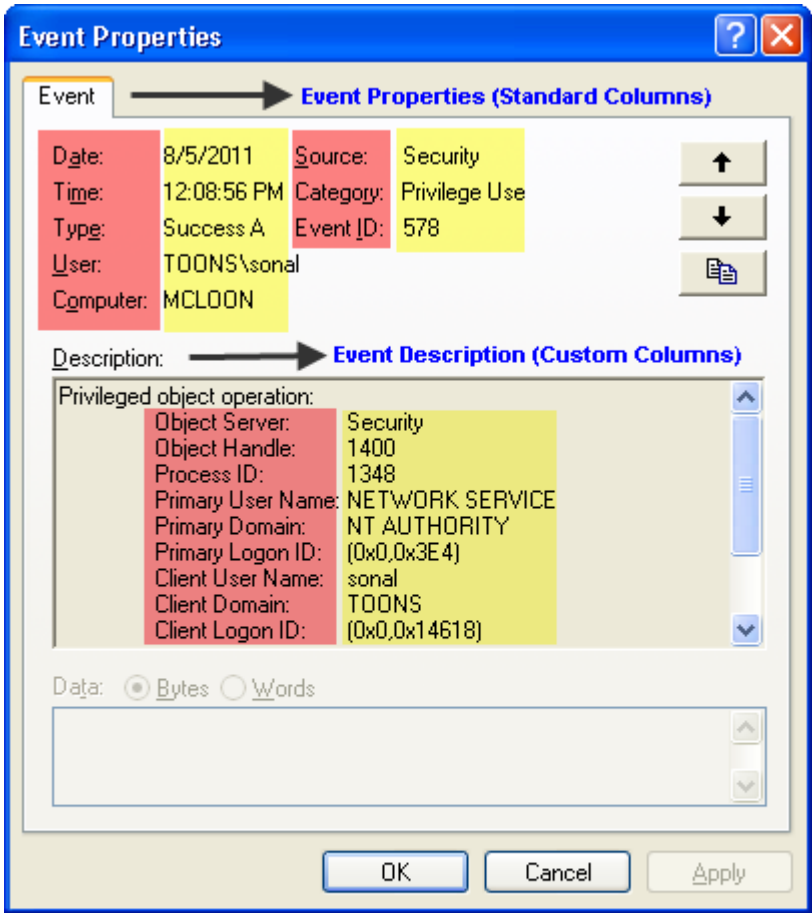
Behavior Rules

Input Rule: Defines what events to consider for behavior analysis. You can define rule to match in Event Properties or Event Description. You can add multiple input rules for 1 custom rule.

Processing Rule: Keyword to look for in the event description. You can choose one from the Custom column list. Custom column list contains selected keywords picked up from the Event Description. You can select only one keyword from the list.

Custom rule is subdivided into three parts: Key, separator, and terminator. Event description is checked for the matching key, then for the separator and terminator, whatever comes in between the separator, and terminator is the text that would be considered for count.

Figure 125
Event Details



Event Properties (Standard Columns)	
Date:	8/5/2011
Time:	12:08:56 PM
Type:	Success A
User:	TOONS\sonal
Computer:	MCLOON
Source:	Security
Category:	Privilege Use
Event ID:	578

Event Description (Custom Columns)	
Privileged object operation:	
Object Server:	Security
Object Handle:	1400
Process ID:	1348
Primary User Name:	NETWORK SERVICE
Primary Domain:	NT AUTHORITY
Primary Logon ID:	(0x0,0x3E4)
Client User Name:	sonal
Client Domain:	TOONS
Client Logon ID:	(0x0,0x14618)

Data: ☒ Bytes ☐ Words

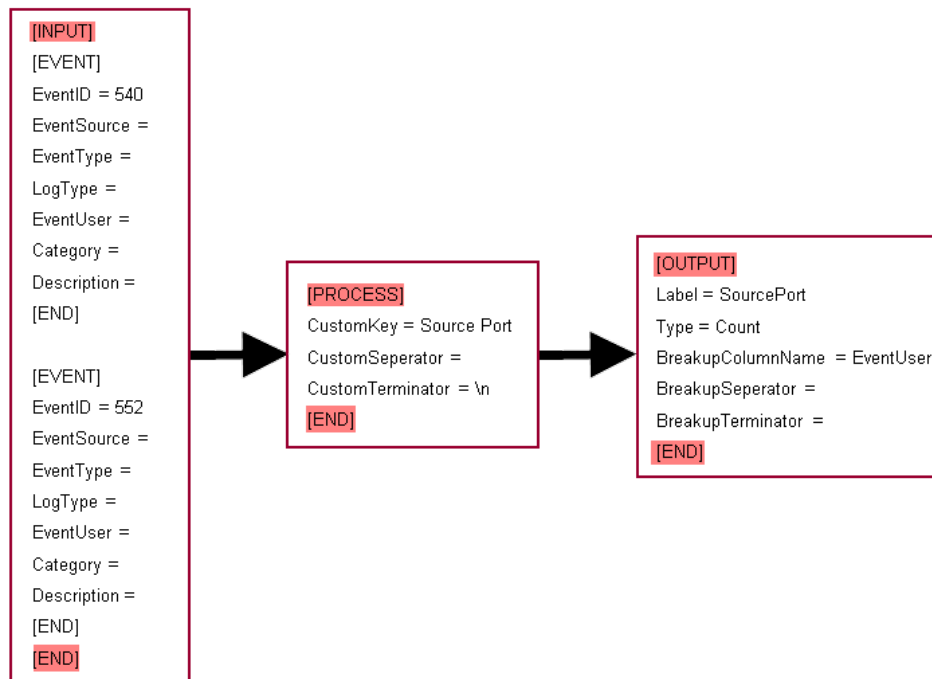
OK Cancel Apply

 ← Column
 ← Value

Display Rule: Defines the display pattern. Display pattern would be Custom column with a breakup column. Breakup column can be one of these: Computer, Event User, Event Source, Event ID or any custom column. You have to specify what breakup column is needed while entering the rule details. You can specify only one breakup column.

Example:

Rule: Process for Source Port



Above mentioned rule tells the 'Enterprise Activity' engine to look for "Source Port" in the event IDs 540 and 552. Maintain a count based on the Event User names. Main breakup would be different Source Ports with their total counts (left pane) and sub-breakup for each Source Port would be the User Names and their counts (right pane).

Managing Behavior Rules

This option helps to set behavioral rules for enterprise activity. You can add these rules as dashlets under **Behavior** → **Security / Operations**.

To set behavior rules

- 1 Click **Admin** hyperlink, click **Control Panel** tab, and then click **Behavior Rules**.
(OR)
Click the **Admin** dropdown, and then click **Behavior Rules**.
EventTracker displays the **Behavior Rules** page with pre-defined rules.

Figure 126
Enterprise Activity
Behavior Rules

Incidents	Status	Behavior	Dashboard	Netflow	Search	Reports	My EventTracker	Change Audit	Config Assessment
Behavior Rules							Page size 25		
Rule Name	Breakup column	Display Name	Active	Delete	For all users	Activation Time			
User Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Admin Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
EventID Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
IPAddress Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
System Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Logon Failure Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Process Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
USB Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
RunAway Process Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Software Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Application Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
							<input type="button" value="Add rule"/> <input type="button" value="Close"/>		

Table 26

Field	Description
Rule Name	Name of the Rule.
Break-Up-Column	Based on this configuration, EventTracker displays the break up details on the Enterprise Activity monitoring page.
For All Users	Select this checkbox for all users to use the Behavior Rule (Dashlet).
Active	Clear this checkbox to inactivate the Behavior Rule (Dashlet).
Display Name	Name of the custom column.

Adding Behavior Rules

This option helps to add behavior rules.

To add behaviour rules

- 1 In **Behavior Rules** page, click **Add Rule**.
EventTracker displays the **Rule Configuration** page.

Figure 127
Event Rule

If the variation percentage value is not specified in **Rule Configuration** page, then the value will be taken from **Admin-> Behavior Settings -> Threshold settings** page, by default.

Rule configuration

Rule name :

☐ Show for all users

Threshold settings

☒ Learn

☐ Custom

Learn Period : mins

Count :

Period : mins

Evaluate Every : mins

☐ Variation : %

☐ Positive ☐ Negative ☒ Both

Event rule

Processing Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
0	0						

AddEditDelete

SaveCancel

'Threshold settings' fields	Description
Learn	Behavior learning period (in minutes). The behavior of custom rule will be monitored for the set learning period and a threshold value will be benchmarked.
Custom	Specify a threshold count for occurrence of the custom rule.
Period	Threshold period in minutes. The custom rule will be monitored for the duration specified in this field. The number of occurrences of custom rule in this duration will be compared with the benchmarked threshold value/ count.
Evaluate Every	The custom rule will be evaluated every 'N' minutes to analyze the activities.
Variation	The variation percentage can be added manually to decide the out of ordinary activities. Positive - If the threshold count observed for the given threshold period is greater than the custom count or learned threshold value then it is considered as positive occurrence of the event rule. If selected, only positive variation activities will be accounted for the analysis. Negative - If the threshold count observed for the given threshold period is lesser than the custom count or learned threshold value then it is considered as negative occurrence of the event rule. If selected, only negative variation activities will be accounted for the analysis. Both - Both the positive and negative variation percentage of the event rule will be analyzed for the selected threshold Period .

If the **Show for all users** option is selected then all the users having administrative privileges can view and edit the rule. If unchecked, only the user who has created the rule can modify it.

2 In the **Rule Name** field, provide a name for the new rule. Ex: Audit Success.

- 3 Check the **Show for all users** option if you wish all users to use this rule.
- 4 In the **Event Rule** tab, click the **Add** button to add event details.

EventTracker displays the **Event Configuration** dialog box.

Figure 128
Add Input Rule

EventTracker considers the event details specified in **Event Configuration** for activity monitoring.

Event Configuration

Log Type : Event Type :

Category : User :

Event Id : Source :

Match in Description : tip

Description exception : tip

To provide special characters like "", "'", "^", "\$", etc. prefix the char with a backslash. Example: \"\\\" for \"\" and \"\\^\" for \"^\".

Add Cancel

- 5 Enter appropriate details in the respective fields, and then click **Add**.

The newly created event rule gets listed on **Event Rule** tab.

- 6 Click the **Processing Rule** tab.

Figure 129
Processing Rule

Event rule

Processing Rule

Display Name	Token	Separator	Terminator
<div> <div>Available list</div> <div>Add new</div> <div>Edit</div> <div>Delete</div> </div>			

Break-up column

Display Name :

Token:

Separator:

Terminator:

Available list

Save

Cancel

 **NOTE**

You can select processing rule from a custom list or you can configure it on your own.

- 7 Select the processing rule from **Available list** or using **Add new** button.

Available list – It is a pre-defined rule set.

Figure 130
Custom Column

	Display name	Token	Separator	Terminator
<input type="checkbox"/>	Accesses	Accesses	:	\n
<input type="checkbox"/>	Authentication Type	Authentication Type	:	\n
<input type="checkbox"/>	Caller Process ID	Caller Process ID	:	\n
<input type="checkbox"/>	Client Domain	Client Domain	:	\n
<input type="checkbox"/>	Client Logon ID	Client Logon ID	:	\n
<input type="checkbox"/>	Client User Name	Client User Name	:	\n
<input type="checkbox"/>	Error Code	Error Code	:	\n
<input type="checkbox"/>	File Object Name	File Object Name	:	\n

Note: Please select a standard or a Token-value

Standard column: Computer Select

Ok Close

Select the checkbox to add a **Token-value** as processing rule, and then click the **OK** button.

These Token-values are extracted from 'Event Description'.

(OR)

Select an appropriate option from the **Standard column** drop-down list.

These column names are extracted from 'Event Properties'.

EventTracker adds the processing rule.

Add new – Add Token-value on your own.

Click the **Add new** button.

EventTracker displays the required fields for you to enter.

Figure 131
Processing Rule

Display Name : Column Name : Separator : Terminator :

Add Cancel

Type appropriately in the relevant fields, and then click the **Add** button.

Figure 132
Processing Rule

Event rule

Processing Rule

Display Name	Token	Separator	Terminator
Windows service	The	SPACE	service

Available list

Add new

Edit

Delete

Break-up column

Display Name :

Token:

Seperator:

Terminator:

Available list

8 Add **Break-up** column details.

Figure 133
Break-up column

Break-up column

Display Name :

Computer

Token:

Computer

Seperator:

Terminator:

Available list

These fields are mandatory. EventTracker considers these details for grouping of events and displays the break up details on the right panes in the **Enterprise Activity Details** page.

9 Click **Save**.

EventTracker displays the **Behavior Rules** page with newly added rule.

Figure 134
Behavior Rules

Behavior Rules

Page size 25

Rule Name	Breakup column	Display Name	Active	Delete	For all users	Activation Time
Windows service activated	Computer	Computer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7/3/2012 12:00:55 PM
User Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
USB Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
System Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Software Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
RunAway Process Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Process Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Network Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Logon Failure Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
IPAddress Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
EventID Activity			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Add rule

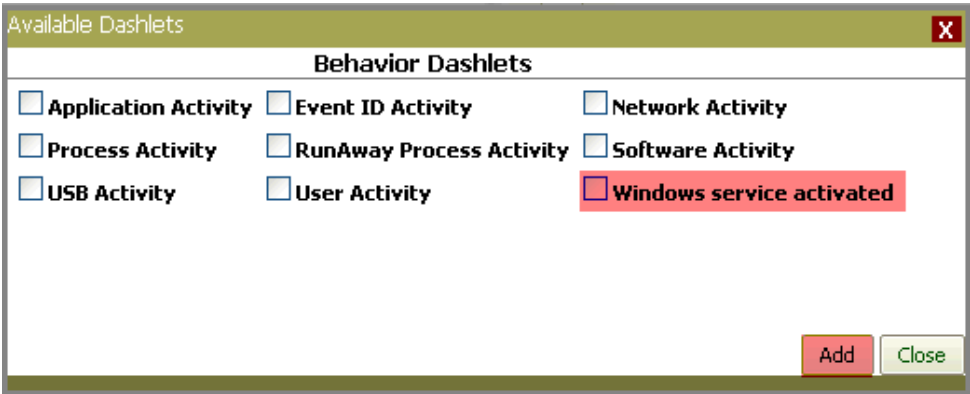
Close

To add custom behavior rule on 'Behaviour' dashboard

- 1 Click **Behavior**, and then click **Security/Operations** tab.
- 2 Select the **Customize** option from the drop-down list.

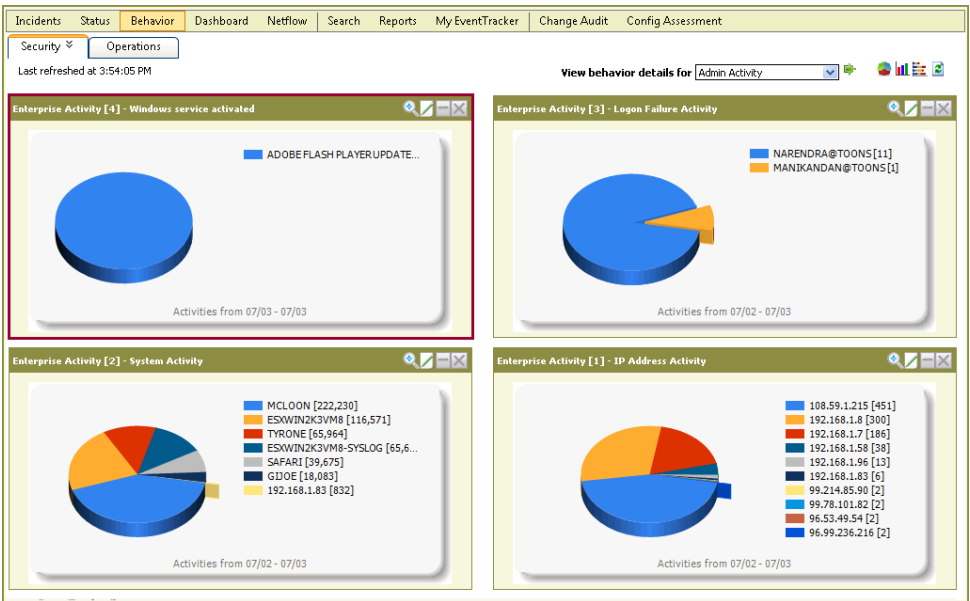
Available Dashlets dialog box displays the newly added behavior rule as a dashlet.

Figure 135
Behavior Dashlets



- 3 Check the newly created behavior rule option, and then click **Add**.
EventTracker displays the dashlet on the **Behavior** dashboard.

Figure 136
Behavior Dashlets



- 4 Click a pie on the chart or a legend to view non-admin user activity details.
EventTracker displays the '**Enterprise Activity Detail**' page.

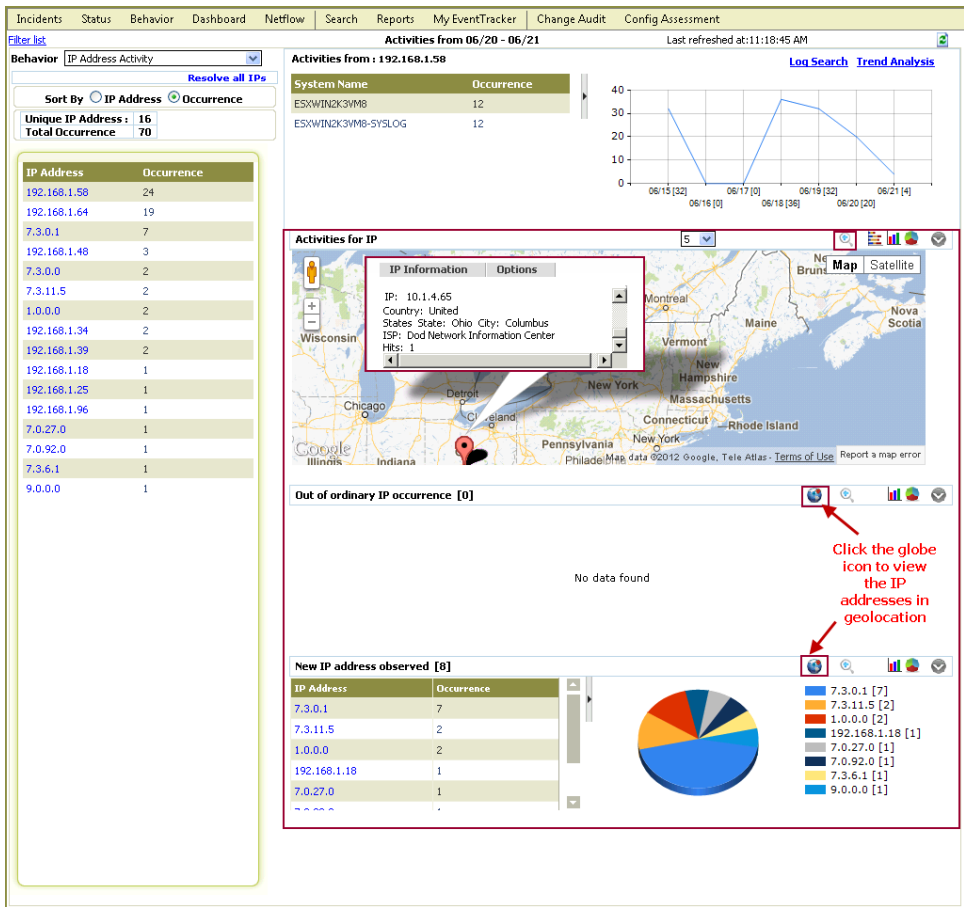
Geo Location

The IP addresses can be located on the map in geolocation. This option is available only for IP address activities. In **Enterprise Activity Details** page, following three panes displays the IP addresses in geolocation:

(Top) Activities for IP

Out of ordinary IP occurrence

New IP address observed



Chapter 5 Dashboard

In this chapter, you will learn how to:

[Keyword Indexed Dashboard](#)

[Viewing Security Dashboard](#)

[Configuring Category Dashlets](#)

Keyword Indexed Dashboard

The Keyword Indexed Dashboard is designed to provide a big canvas for the user to add custom dashlets in the dashboard. The user is allowed to use standard columns (i.e. Event ID, Event User, Computer, Event Source, Domain, Event Type, and Event LogType)/ category/ keywords to configure the dashlets to be added in the dashboard. The selected keywords/standard columns will be displayed as a trend graph in the dashboard.

EventTracker provides three types of dashboard: Security, Operations, and Compliance

The process to configure and customize the dashlets is identical for **Security** and **Operations** dashboard. For **Compliance** dashboard, the dashlets cannot be configured and customized. It displays %\$%\$%^ in the in-built dashlets.

Features of keyword indexed dashboard:
User can edit or delete the configured keyword dashlets.

A customized selection of standard column properties or keywords or categories can be used to create a dashlet.

The configured dashlets can be viewed by different graph types. The zoom preview of graph is also possible.

The graph will take you to log search page for the selected entity.

Dashlets configured in Security/Operations are made available to all the users enterprise wide and those configured in My EventTracker is made available to a user who has created them.

Viewing Security Dashboard

This option helps to view quick statistics like trend of events occurred and summary on event categories.

To view security Dashboard

- 1 Log on to **EventTracker Enterprise**.
- 2 Click **Behavior**, and then click the **Security** tab.

By default, EventTracker displays past 6-hour trend of Security: Logon failure events, and Security: User logon events.

Figure 137
Security Dashboard
- Trend

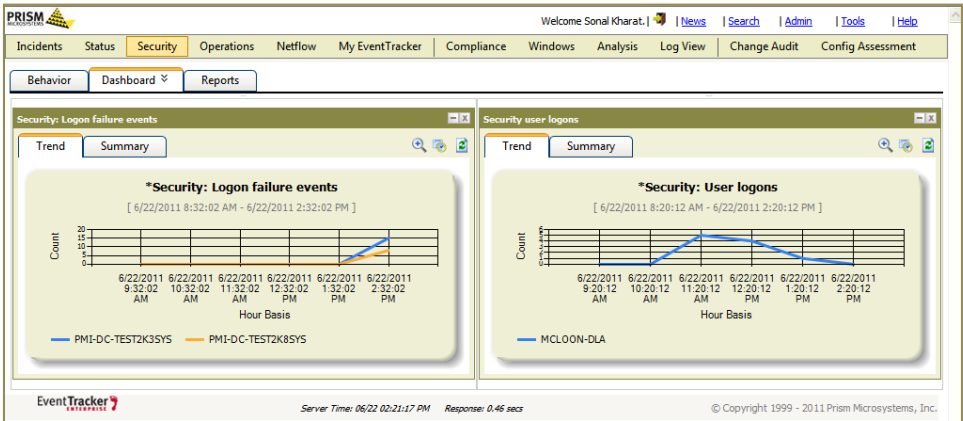
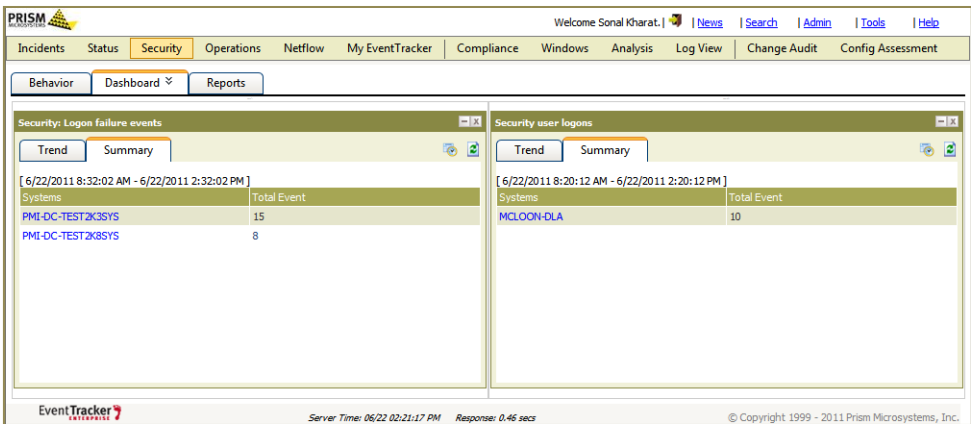


Table 27

Click	To
	Zoom the graph.
	Reconfigure the Dashlet. While reconfiguring, you can reset the Time Range and Refine & Filter criteria.
	Refresh the Dashlet with latest events.
	Minimize the Dashlet.
	Maximize the Dashlet.
	Dismiss the Dashlet.

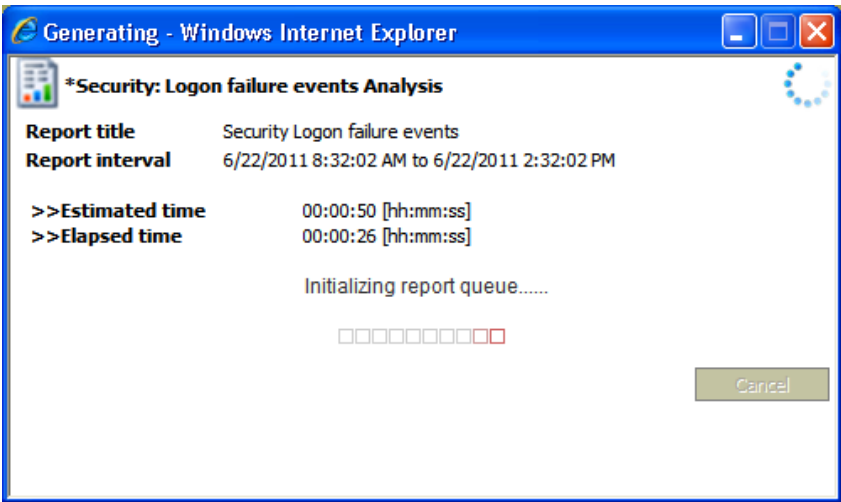
3 Click the **Summary** tab to view summary report.

Figure 138
Security Dashboard
- Summary



4 Click the hyperlink in the **Systems** column to generate detail report.
EventTracker displays the report generation progress bar.

Figure 139
Progress bar
depicting report
generation



After successful generation, EventTracker displays the detail report in the Smart Viewer.

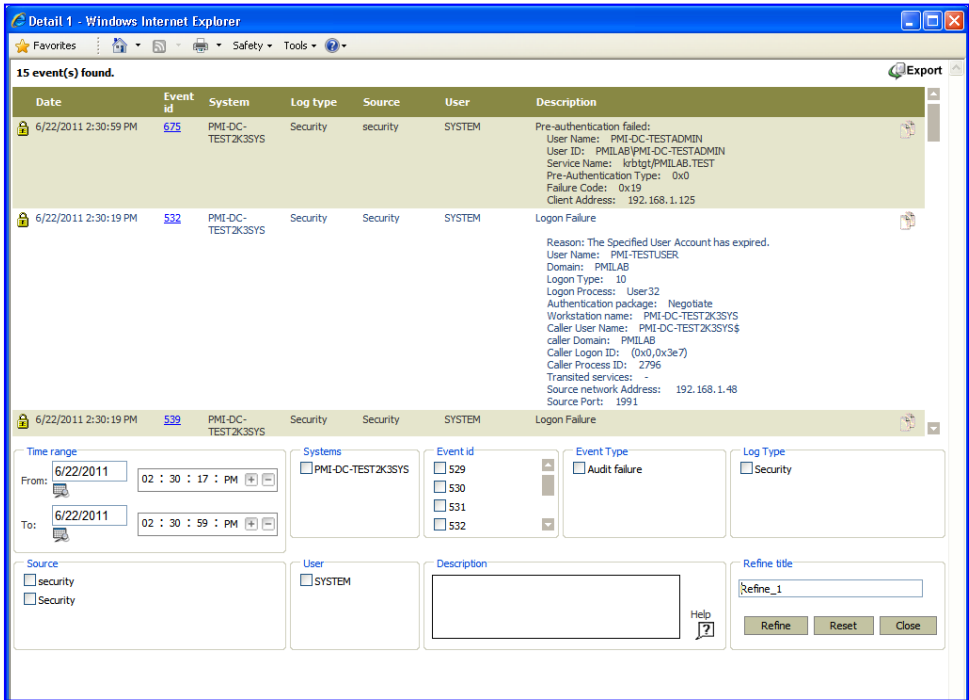


Figure 140
Smart Viewer

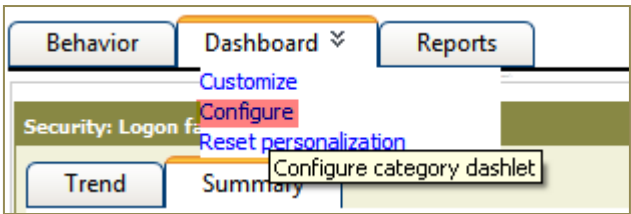
Configuring Category Dashlets

This option helps to configure Category Dashboard Dashlets.

To configure Category Dashboard Dashlets

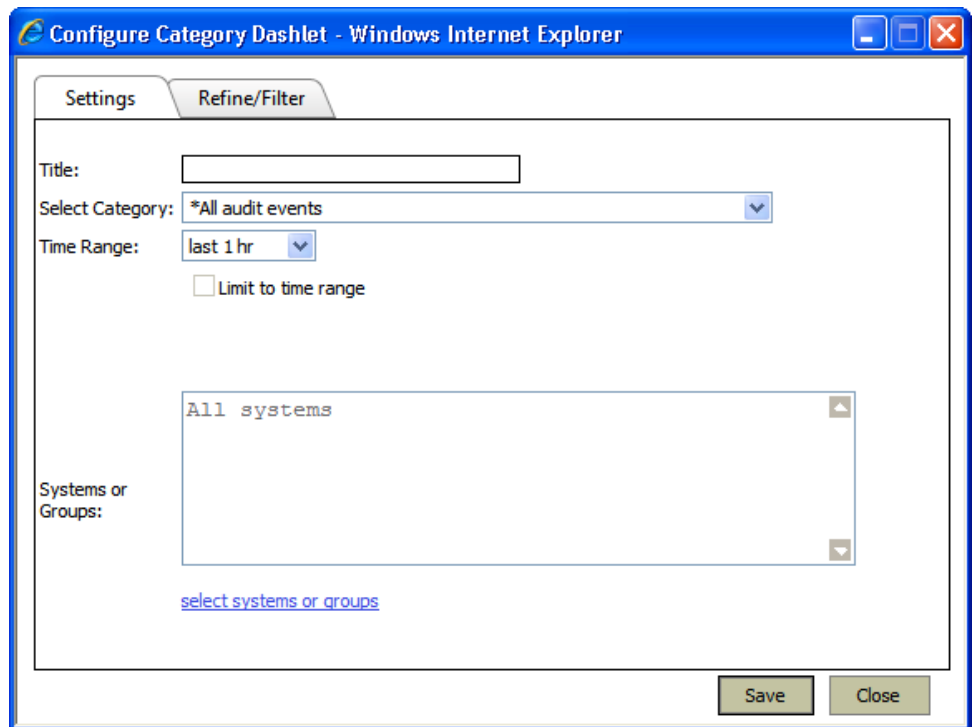
- 1 Log on to **EventTracker Enterprise**.
- 2 Click **Security**.
- 3 Click **Dashboard**.

Figure 141



- 4 Click the **Configure** hyperlink from the drop-down list.
EventTracker displays the Configure Category Dashlet window.

Figure 142
Configure Category
Dashlet



Configure Category Dashlet - Windows Internet Explorer

Settings Refine/Filter

Title:

Select Category: *All audit events ▼

Time Range: last 1 hr ▼

☐ Limit to time range

Systems or Groups: All systems

[select systems or groups](#)

Save Close

- 5 Type the title of the Dashlet in the **Title** field. Ex: Syslog Events
- 6 Select a Category from the **Select Category** drop-down list.
Ex: *All Syslog events
- 7 Select the **Time Range**.
- 8 Select the **Limit to time Range** checkbox, if you wish to monitor events occur during that time period.
- 9 Set the time range.

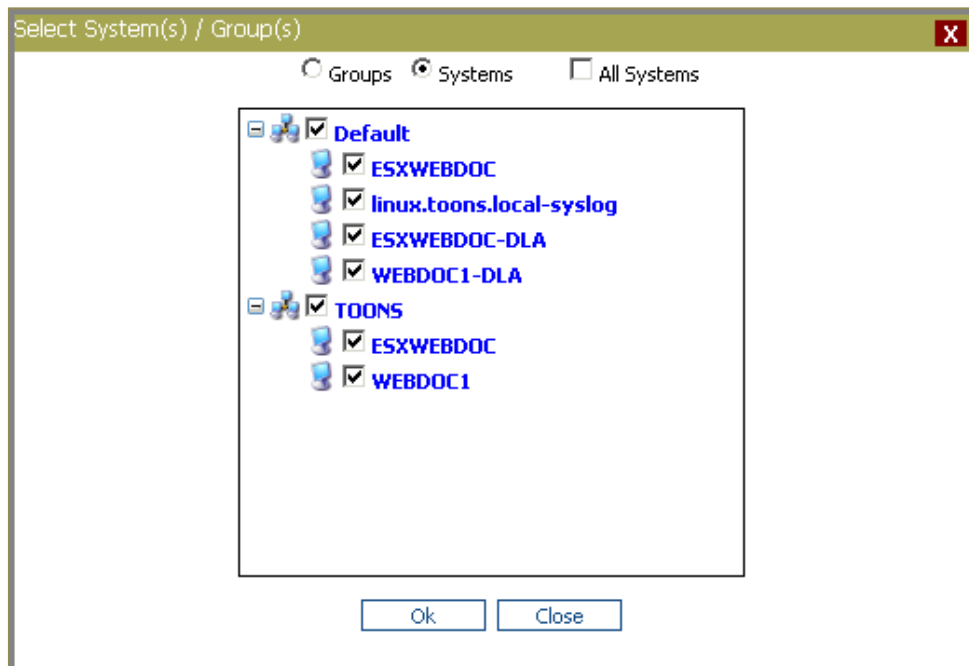
Figure 143
Configure Category
Dashlet – Refine/
filter

NOTE

EventTracker enables the Limit to time range checkbox only when you select last 1 day, last 2 days, or last 1 week options.

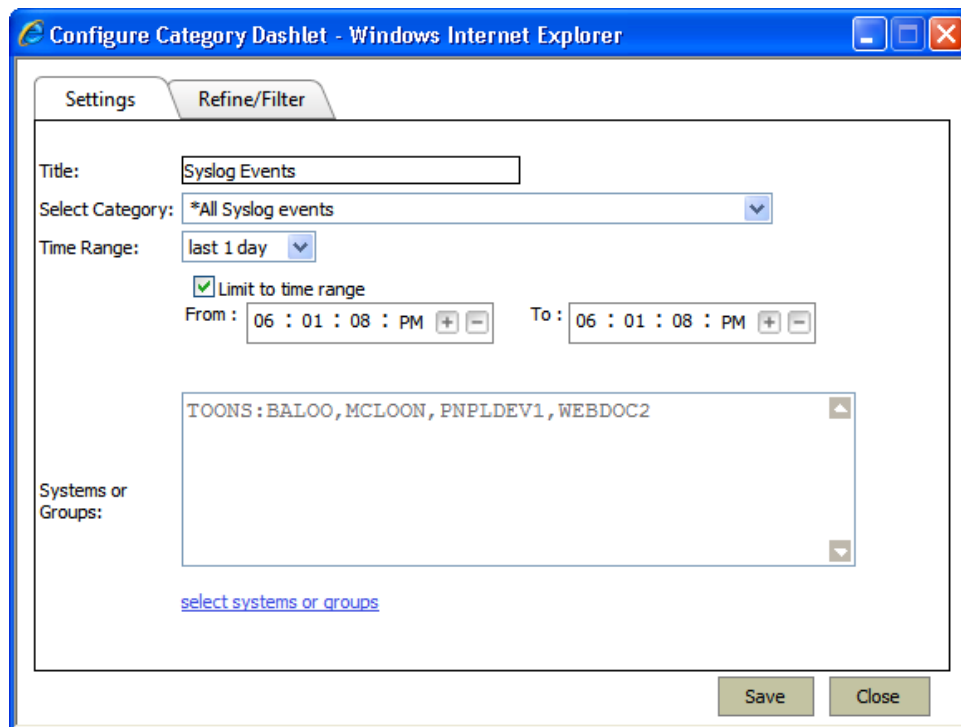
- 10 Click **select systems or groups** to configure the Dashlet for specific systems / groups.
EventTracker displays the Select System(s) / Group(s) window.
By default, EventTracker selects all managed systems.

Figure 144
Configure Category
Dashlet



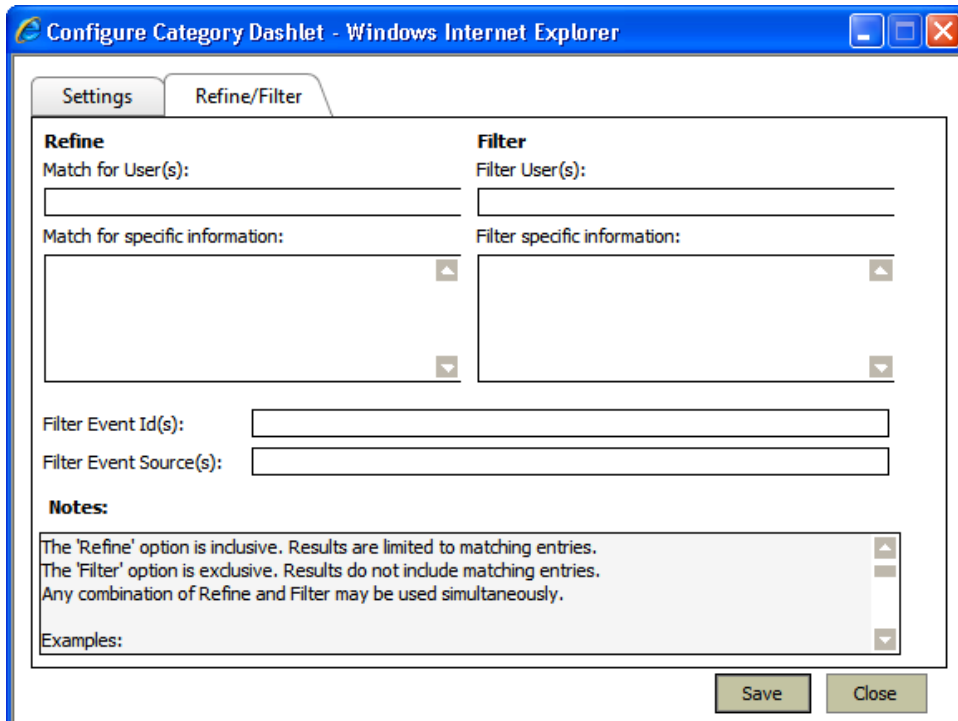
11 Select the system(s) / Group(s) and then click **OK**.

Figure 145
Configure Category
Dashlet



- 12 Click the **Refine/Filter** tab.

Figure 146
Configure Category
Dashlet



- 13 Set the **Refine/Filter** criteria to narrow down your query.
- 14 In **Filter Event Id(s) /Filter Event Source(s)** field, enter the Event Id(s)/ Source(s) that you do not wish to see in the generated report.
- 15 Click **Save**.

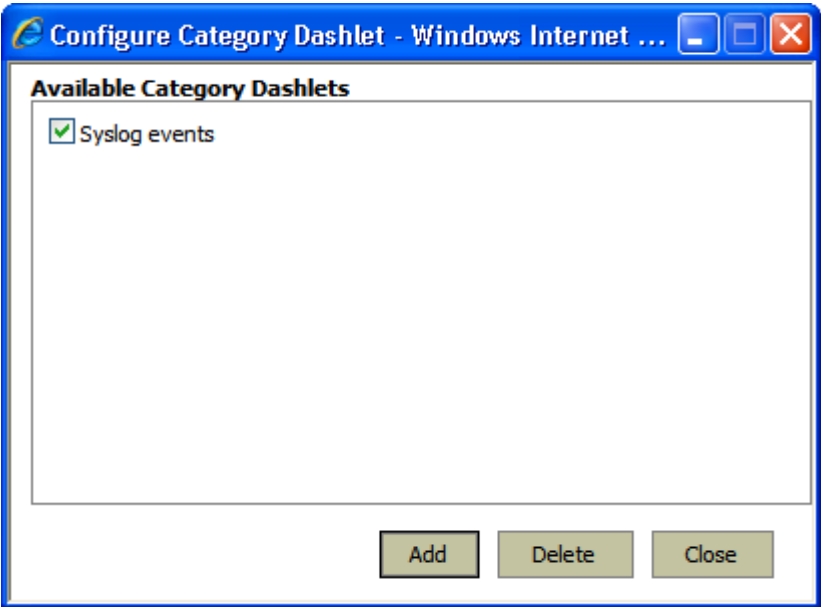
Customizing Security Dashboard

This option helps to customize the Security Dashboard.

To customize the security dashboard

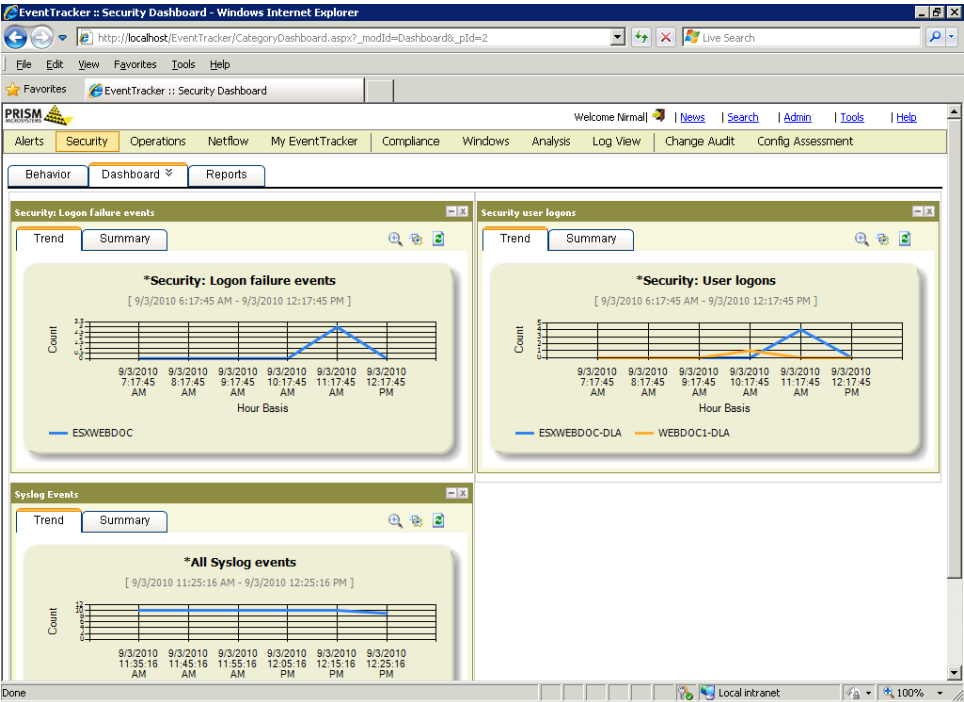
- 1 Click **Dashboard**.
- 2 Click the **Customize** hyperlink.
EventTracker displays **Configure Category Dashlet** pop-up window.
'Configure Category Dashlet' displays only configured categories.

Figure 147
Configure Category
Dashlet



- 3 Select the checkbox against the Dashlet, and then click **Add**.
EventTracker adds the Dashlet to the Dashboard and displays the trend of events of the selected Category.

Figure 148
Security -
Dashboard



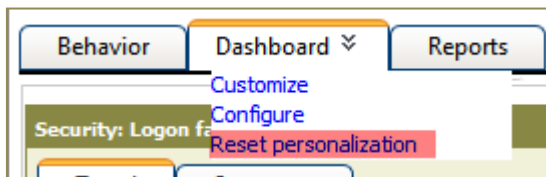
Resetting Personalization

This option helps to reset the dashboard with default dashlets.

To reset personalization

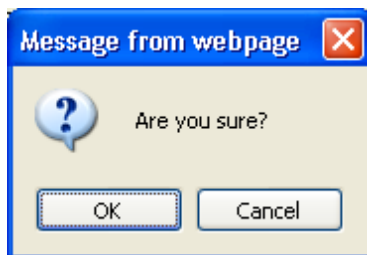
- 1 Click **Dashboard**.

Figure 149



- 2 Click the **Reset personalization** hyperlink.
EventTracker displays the confirmation message box.

Figure 150



- 3 Click **OK** to reset the dashboard.
EventTracker removes the custom dashboard that you have added.

Compliance Dashboard

Compliance Dashboard gives you the overview of Organization /Enterprise's status with respect to compliance. This dashboard can be used to track the compliance readiness of the Organization/Enterprise.

If user marks an Alert to be shown in Compliance Dashboard, and if an incident is generated, based on that alert, then that Incident will be shown in **Compliance Dashboard**.

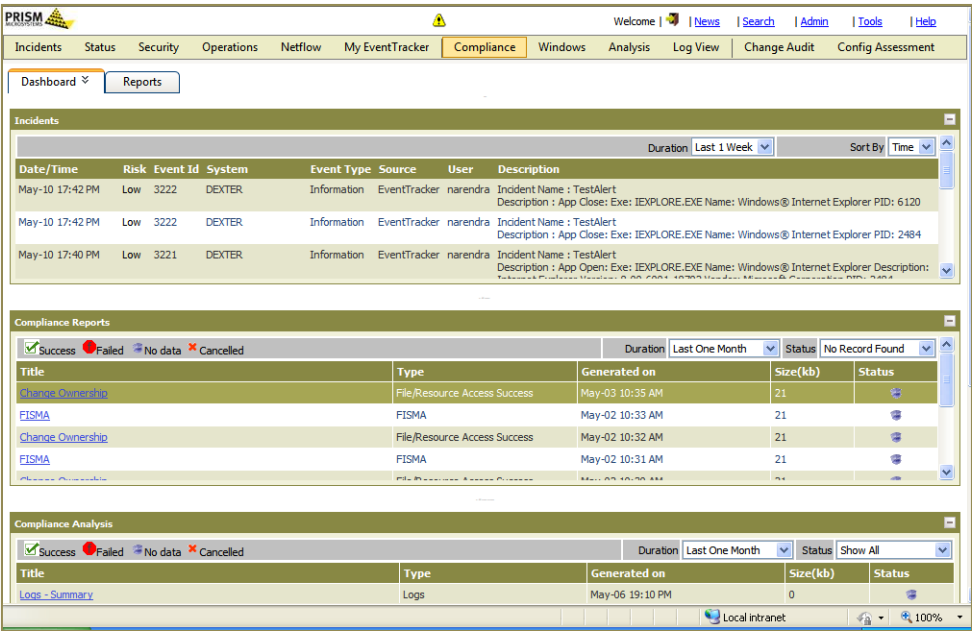
Compliance Dashboard comprised of 4 dashlets:

- 1 **Incidents:** The results of the Incidents.
- 2 **Compliance Reports:** The results of the Compliance reports.
- 3 **Compliance Analysis:** The results obtained from Analysis.

Note: Only On Demand, Queued and Scheduled reports can be added to Compliance dashboard.

4 **Config. Assessment:** Config. Assessment results (i.e. the reports that are generated under Config. Assessment).

Figure 151
Compliance
dashboard

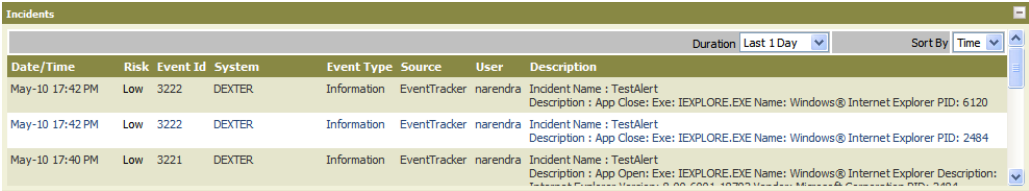


1 **Incidents Dashlet**

Incidents Dashlet gives the list of incidents related to compliance.

Please read [Adding custom Alert](#) to know how the incidents appear in the compliance dashboard.

Figure 152
Incidents Dashlet



2 **Compliance Reports**

Reports generated through 'Compliance Reports' will reflect in **Compliance Reports** Dashlet.

Figure 153
Compliance reports
dashlet

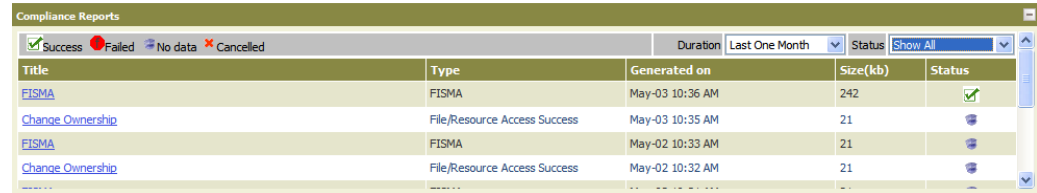






Table 28






Select	For
--------	-----

 Success	Successful Reports
 Failed	Failed Reports
 No data	Report with no data
 Cancelled	Reports that are cancelled by the user/machine or by the EventTracker itself.

3 Compliance Analysis

If while generating Analysis, ‘Show in: Compliance Dashboard’ option is selected then the generated analysis will be displayed in the **Compliance Analysis** dashlet. With the help of Compliance Analysis, user can identify any areas of non-compliance and make the necessary amends.


Figure 154
Compliance Analysis dashlet

Compliance Analysis				
 Success  Failed  No data  Cancelled				
Duration		Last One Month		
Status		Show All		
Title	Type	Generated on	Size(kb)	Status
Logs - Summary	Logs	May-06 19:10 PM	0	

4 Configuration Assessment

In **Configuration Assessment**, whichever reports are generated with respect to a benchmark, they are shown in the **Configuration Assessment** dashlet.

Figure 155
Config Assessment dashlet

Config Assessment								
 Success								
Duration		Last 1 Day						
Status		Success						
Title	Benchmark Title	System	Generated on	Passed	Failed	Exceptions	Deviations	Result File
Test2	MS-SCM Win XP SP3 (EC-Desktop)	MCLOON	Jun-23 14:06 PM	39	83	0	0	View
Test	MS-SCM Win XP SP3 (EC-Desktop)	MCLOON	Jun-23 11:43 AM	39	83	0	0	View

NOTE

You can minimize and reshuffle the sequence of dashlets by dragging the dashlet to desired place.

Chapter 6

Reports

In this chapter, you will learn how to:

- [Generate Alphabetical Reports](#)
- [Generate Security/Operations/Compliance Reports](#)
- [Generate My EventTracker Reports](#)
- [Configure Enterprise Feeds](#)
- [Configure My Feeds](#)
- [Interpret Reports Exceptions](#)
- [Use Refine & Filter Criteria](#)
- [Scheduled Reports](#)
- [Defined / Scheduled Reports Using Existing Configuration](#)
- [View Scheduled Reports History and Details](#)
- [Send Published Reports via E-mail](#)
- [Run Scheduled Reports On Demand](#)
- [Generate On Demand Reports – Foreground](#)
- [Generate On Demand Reports – Foreground – Power Viewer](#)
- [Generate On Demand Reports – Foreground – Smart Viewer](#)
- [Generate On Demand Reports – Background \(Queued\)](#)
- [Defined Reports](#)
- [Use Report Calendar](#)
- [Use Report Status Snapshot](#)
- [Add Favorites](#)
- [View Favorites list](#)

Alphabetical Reports

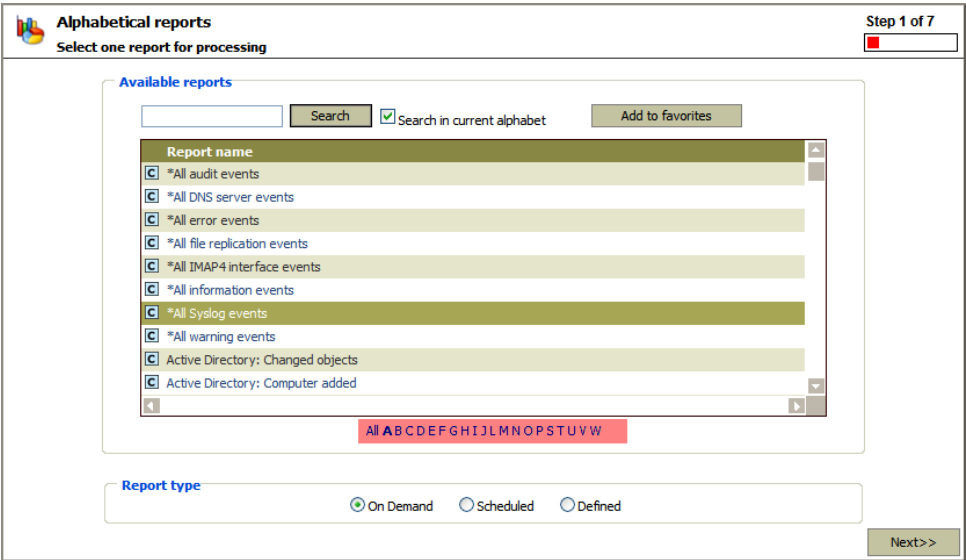
Reports are arranged in alphabetical order to easily spot and configure On demand, Scheduled, and defined reports. Icons C, R, and A represent, Categories, Miscellaneous Reports, and Analysis respectively. Search option is provided to enter a free-form search query.

To access Alphabetical Reports

- 1 Click **Reports**, and then click **Alphabetical Reports**.

EventTracker displays the 'Alphabetical reports" page.

Figure 156
Alphabetical Reports




- 2 Click the alphabet hyperlink to view appropriate Category/Report/Flex Report list.

(OR)

Type the search phrase in the search field, click the **Search in current alphabet** checkbox, and then click **Search**. Example: alert

EventTracker displays the Category/Reports/Flex Report searched for.

Note 

Search in current alphabet checkbox is not enabled when you click All hyperlink.

- 3 Select a Category/Report/Flex Report from **Report name** column.
- 4 Click **Next>>**.

EventTracker displays the Reports Wizard.

Note 

You can also add Category/Reports/Flex Report to the favorites list. To do this select a Category/Reports/Flex Report and then click **Add to favorites**.

Security/Operations/Compliance and My EventTracker Reports

Any user who has access to EventTracker can configure and view the Security, Operations, and Compliance reports.

My EventTracker Reports can be configured and viewed only by the owner who configured those reports. No other user can view or modify My EventTracker Reports. However, the administrator can view the configured reports and not the generated reports.

Procedure to configure On Demand, Queued, Scheduled, and Defined reports are identical for Security, Operations, Compliance, and My EventTracker Reports.

Security/Operations/Compliance Reports

Security

Reports that show the occurrence of various security related events across systems, devices, and applications. These may be generated and reviewed on a regular schedule to pinpoint potential risks or breaches.

Useful to decisively counter the internal and external security threats.

Operations

System health monitoring is an important benefit of event log management. These reports are useful to observe anomalies in system performance (CPU, disk, memory), service failures, network connections, printer usage etc.

In addition, EventTracker has now added new reports under 'EventTracker'. Those are 'EventTracker Admin Activity', 'EventTracker Correlation Events', and 'StatusTracker Resource Summary'. These reports will help you,

- To track all EventTracker configuration changes that have been made by the user.

- To show the correlated events for a given time period and for a selected correlation rule.

EventTracker Admin Activity:

[Operations > EventTracker > EventTracker Admin Activity](#)

This report gives you information on the configuration changes in EventTracker or selected Categories in your enterprise. The report can be used to track 'system activity' in relation to a selected Category or changes done in the 'EventTracker application' configurations, thereby giving you an insight into the security and other implications.

EventTracker Correlation Events:

[Operations > EventTracker > EventTracker Correlation Events](#)

This report gives you the correlated events for a given time period and for a selected correlation rule. While generating a report, user can select only one correlation rule (multiple selection not allowed), systems, and time duration for the report. The report engine will fetch the data for the given criteria and match the correlation rule(s).

The report should provide details of how many times the correlation rule(s) matched in the given criteria and list the matching events.

StatusTracker Resource Summary

[Operations > StatusTracker Resource Summary > Application Resources](#)

This report summarizes the status of monitored applications for the selected period.

[Operations > StatusTracker Resource Summary > System Resources](#)

This report summarizes the status of monitored systems for the selected period.

Compliance

Reports that show the compliance posture of enterprise assets, these are helpful to demonstrate alignment with standards.

Security/Operations/Compliance Reports page encompasses Tree pane, Actions Pane, Summary pane, and Details pane.

Navigation Tree is an assortment of predefined report types. Reports of same type are grouped together for faster identification and navigation. Expand the nodes to select a report type that you wish to generate.

Actions pane contains related actions you can perform on the report type you have selected in the tree pane.

EventTracker displays summary in the upper pane of the Dashboard on all generated On Demand, Queued, and Scheduled reports.

Table 29

Field	Description
Title	Name of the report.
Type	Formatting option of the report..
Generated on	Date and time when the report was generated.
Size(kb)	Size in KB of the report.
Report Status	Status of the report such as Success, Failed, No data and Cancelled.
Filters: You can use Duration or Status or combination of both to narrow down your search criteria.	
Display	Available options Summary and Exception. Summary is selected by default. Select Exception to move through the Exceptions page.
Duration	Available options are Last One Hour, Last One Day, Last One Week and Last One Month.
Status	Available options are Show All, Success, Failed, and No Record Found.

To see the configuration details and exception details of the report,

- 1 Click **Compliance >> Reports >> Actions pane >> Dashboard**.
Reports Details pane is selected by default.
- 2 Click the **Exception details** tab to view the exception summary of the selected report.

Note



In the Top pane, click the title hyperlink to view the report configuration in PDF format.

My EventTracker Reports

My EventTracker Reports page encompasses Tree pane, Actions Pane, Summary pane and the Details pane.

Navigation Tree is an assortment of predefined report types. Reports of same type are grouped together for faster identification and navigation. Expand the nodes to select a report type that you wish to generate.

Actions pane contains related actions you can perform on the report type you have selected in the tree pane.

EventTracker displays summary in the upper pane of the Dashboard on all generated On Demand, Queued and Scheduled reports for the tab (Compliance, Security, Operations) selected.

Searching Security/Operations/Compliance/My EventTracker Reports

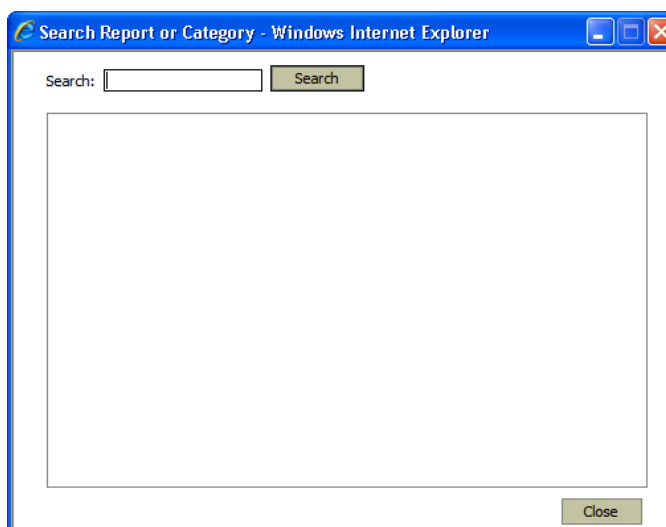
This option helps you search report or category.

To search report or category

- 1 Click the search  icon on the **Reports** tab.

EventTracker displays the **Search Report or Category** window.

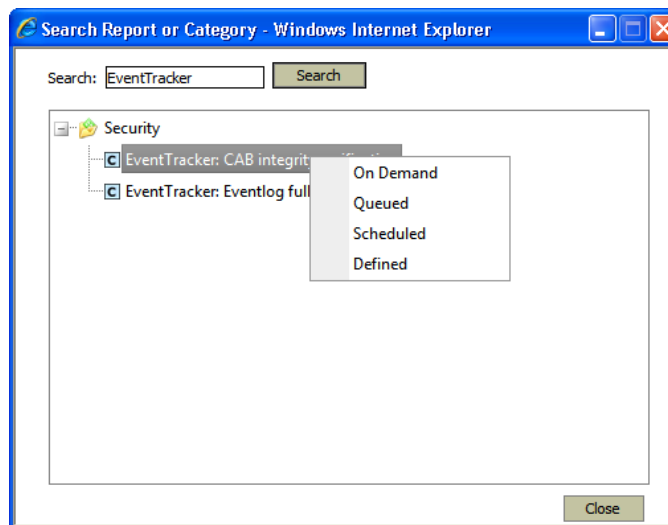
Figure 157
Search Report or
Category



Search is case insensitive; however, you cannot use wild cards to search report or category.

- 2 Type the name of the report or category in the **Search** field, for example "EventTracker"
- 3 Click **Search**.
EventTracker displays the search result.
- 4 Right-click the report or category.
EventTracker displays the shortcut menu.

Figure 158
Search Report or
Category



- 5 From the shortcut menu, choose an appropriate option.

Enterprise Feeds

Enterprise Feeds can be configured and linked with Compliance, Security, and Operations Reports to send RSS notifications when the Scheduled Reports are generated. Any user can use these feeds and can also be linked with My EventTracker Reports.

To view Enterprise Feeds

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** dropdown, and then click **RSS**.

EventTracker displays the 'RSS Feeds' page.

For more information of configuring Enterprise Feeds, refer [Chapter 14 Configuring RSS Feeds](#)

My Feeds

My Feeds can be configured and linked with My Reports to send RSS alerts when the scheduled My Reports is generated. My feeds are exclusive to the users who configure them.

To add My Feeds

- 1 Log on to EventTracker Enterprise.
- 2 Click **My EventTracker**.
- 3 Click **Reports**.
- 4 Click **My Feeds** on the Actions pane.
EventTracker displays the 'My Feeds' page.

Table 30
Field Description

Field	Description
Feed Name	Name of the RSS Feed.
Description	Short description of the feed.
RSS Link	Link generated by EventTracker.
RSS	Copy the link in this column and add the same in the RSS Reader to receive notification.
Reports Linked	Click the links to view the reports linked with their corresponding feeds.
Edit	Click the links in this column to edit the feed.
Active	Displays the Active/Inactive status of RSS link.
Delete	Select the checkbox to delete the feed.
Add New	Click to add RSS Feeds.
Delete	Click 'Delete' button to delete the selected feed.

- 5 Click **Add New** to add new feeds.
 - 6 Type appropriate details in the relevant fields.
 - 7 Click **Save**.
-

Reports Wizard

Reports Wizard has been designed to simplify the report generation and scheduling process by guiding you through a set of steps. You can select the report type, the systems, the time period and options and the data filters (if any).

Reports can be generated in PDF, HTML or WORD formats.

After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.

Reports Exceptions



Exceptions that occurred during report generation are displayed in this page. You can also add and clear follow up notes for the exceptions. Filtering options are provided to narrow down your search criteria.

- 1 Log on to EventTracker Enterprise.
- 2 Click **Reports**.
- 3 Click **Compliance / Security / Operations / My EventTracker**.

By default, EventTracker selects the first record in the top pane and displays the corresponding details in the bottom pane.

- 4 Click the **Exception Details** tab on the bottom pane.
EventTracker displays the Exceptions details of the selected record.
- 5 To view all exceptions, click **Exceptions** on the Actions pane.
EventTracker displays the 'Exceptions' page.


Table 31
Field Description

Field	Description
Exceptions	
Generated on	Date and time when the exception had occurred.
Exception name	Name of the exception.
Exception details	Summary of exception
Filter: You can use either one or both of these filter options.	
Duration	Available options are Last One Hour. Last One Day. Last One Week. Last One Month. Select an option from this drop-down list to view respective exceptions.
Exception Type	Available options are Show All, flagged, Unflagged.  Represents Flagged exceptions. Flagged are ones that are with unattended comments.  Represents Unflagged exceptions. Unflagged exceptions are ones that are with acknowledged comments or no comments.


Exceptions are raised under the following circumstances:

- Report generation fails.
- Report-processing time exceeds maximum allowed time (1 hour).
- E-mail fails.

Flagging for follow up

- Click  .
EventTracker displays the Add Notes window.
- Type the follow up note in the **Add new note** field and then click **OK**.

Clearing / acknowledging flags

- Click  .
EventTracker displays the 'Add Notes' window.
- Type the follow up note in the **Add new note** field and then click **OK**.
Notes entered earlier are displayed in the 'Notes' field.

Refine & Filter Options

Refine and Filter options in the Reports Wizard helps you to narrow down your filtering criteria while configuring reports.

Table 32
Field Description

Field	Description
Refine: Use this option if you are looking for specific information.	
Match for User(s)	This field can take multiple strings separated by . Stands for OR condition. Example- If you wish to generate a Log on/off Activity report for a specific user named "John" then, just enter John in the 'Match for User(s)' textbox. If you are looking for multiple users John, Leonard and Susan then, enter as John Leonard Susan.
Match for specific information	This field can take multiple strings separated with && or . && Stands for AND condition and stands for OR condition. If you want to make a match on any of the special characters like "\", "^", "\$", etc., then in the search string prefix this char with a backslash, like "\\\" for a "\" and "\\^\" for a "^". Example- If you wish to generate a Printer Usage report for a specific printer named "FLR1PRINTER" then, just enter FLR1PRINTER in 'Filter for Specific Info' textbox. If you are wish to generate a Printer Usage report for a specific user "Susan", specific printer "FLR1PRINTER" and specific document "FinancialInfo.xls", you have to enter Susan in 'Match for User(s)' textbox and you have to enter FLR1PRINTER&&FinancialInfo.xls in 'Filter for Specific Info' textbox.
Filter: Use this option if you want to ignore specific information.	
Filter User(s)	Type the user names to exclude from report generation.
Filter specific	Type the information that you want to filter out in this field.

Field	Description
information	Example- Suppose you want to generate software usage for a use and want to exclude all Microsoft applications from the report. Just enter Microsoft in this field.
Use this option if you do not wish to see specific Event Id(s) or Event Source(s)	
Filter Event Id(s)	Enter the Event ID(s), which you do not wish to see in the report. Use as a separator to enter multiple event Id(s).
Filter Event Source(s)	Enter the Event sources(s), which you do not wish to see in the report. Use as a separator to enter multiple event Id(s).

Scheduling Reports

To configure Scheduled Reports

- 1 Log on to EventTracker Enterprise.
- 2 Click **Reports**.
- 3 Click **Compliance / Security / Operations**.
(OR)
Click **Reports**.
Click **My EventTracker**.
Click the **Compliance / Security / Operations** tab.
- 4 Expand a node and select a report type.
- 5 Click **Scheduled** on the Actions pane.
EventTracker displays the Reports Wizard.
(OR)
Right-click a report.
EventTracker displays the shortcut menu.
From the shortcut menu, choose **Scheduled**.
EventTracker displays the ‘Scheduled’ page.

Table 33
Field Description

Field	Description
Overview	
Notes	Click the icon to add or view review notes.
Title	Name of the report. Click the title of the report to view the report.
Created on	Date and time when the report was created.

Table 34
Field Description

Field	Description
Size(kb)	Size in KB of the report.
Status	Status of the report such as Success, Failed and No record found.






Click	To
Overview	
	Search published reports.
	Refresh the pane.
	Export the list of generated scheduled reports in to Excel format.
 Show all	Display all the scheduled/queued/defined report & analysis in the Reports dashboard.

Table 35
Field Description

Field	Description
Scheduled	
	Indicates that e-mail is configured.
Title	Name of the report.
Scheduled by	Name of the user who configured the schedule.
Type	Type of the report.
Frequency	How often the report is generated.
Next Run	Date and time when the report will run next.
Scheduled on	Date and time when the schedule was configured.
Feed	RSS Feed linked with the schedule.
Status	Date and time when report was generated in the immediate past and the healthy status of the report.

If there are no reports scheduled or generated, then EventTracker displays the page with empty panes.

When no records are found, then EventTracker will not generate the output. To create a dummy PDF for the reports with no records, you need to select the **Generate default report in case of no matching record found** checkbox in the configuration page.(by default the option is enabled in Admin->report settings)

Note



If the user disables the option then the pdf report will not get generated when no records are found.

- 6 Click **New** in the Scheduled pane.
EventTracker displays the Reports Wizard.
- 7 Click **Next >>**.
- 8 Select the **Categories** (when applicable) and then click **Next>>**.
- 9 Select Sites/Systems/System Groups.
- 10 Click **Next >>**.
- 11 Set the **Scheduled Type**. Available options are Daily, Twice Daily and Weekly.

Note



If you select **Daily** and **Weekly** as Scheduled Type, EventTracker displays the **Limit to time range** checkbox. By selecting this checkbox, EventTracker enables **From** and **To** spin boxes. Set the time range for EventTracker to consider events occurred during that period alone.

- 12 Set the **Start Time**. Example: 12:00:00 PM

Note



EventTracker enables **Week Day** drop-down list only when you select **Weekly** option as Schedule Type.

- 13 Select an appropriate **Format option** (when applicable). Available options are Summary, Extended Summary, Details and Trend Analysis.
- 14 Select an appropriate **Export type** option. Available options are PDF, WORD and HTML.
- 15 Select an appropriate **Chart type**. Available options are PIE, BAR, LINE and NONE.
- 16 Select an appropriate **Sort by** option.
- 17 Click **Next >>**.
- 18 Type appropriate **Refine, Filter** options and then click Next >>.
- 19 Type the **Title, Header, Footer** and **Description**.
- 20 Click **Next >>**.
- 21 Crosscheck the Disk cost analysis details.
- 22 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail. Type valid recipient **E-mail** address.
- 23 Select a RSS Feed from the **Update status via RSS** to receive RSS notification drop-down list.

- 24 If you wish to add the report in compliance dashboard, then select 'Compliance Dashboard' from **Show in** dropdown.
 - 25 Click **Next >>**.
 - 26 Crosscheck the configuration and then click **Schedule**.
EventTracker adds the new schedule to the Scheduled pool.
-

Defining / Scheduling Reports Using Existing Configuration

You can **Define** or **Schedule** reports/analyses with the same configuration settings of generated reports/analyses. To do this, select a generated report in the top pane and then select an appropriate option from the **Use Configuration** drop-down list. EventTracker starts the Reports Wizard.

To define / schedule reports using existing configuration

- 1 Click **Compliance / Security / Operations**.
 - 2 Click **Reports**.
(OR)
Click **My EventTracker**.
Click **Reports**.
Click the **Compliance / Security / Operations** tab.
EventTracker displays the Dashboard.
 - 3 Select a generated On Demand report in the top pane.
EventTracker displays the corresponding details in the bottom pane.
 - 4 Select an appropriate option from the **Use configuration** drop-down list.
Example: Create defined report.
 - 5 Click **GO**.
EventTracker starts the Reports Wizard.
-


Viewing Scheduled Reports History and Details

To view scheduled reports history and details

- 1 Click **Scheduled** on the Actions pane.
EventTracker displays the Scheduled page.
- 2 Click a title of the scheduled report in the bottom pane.
EventTracker displays the Report configuration details in the **Report details** tab.
- 3 Click the **History** tab to view report generation history.
- 4 Click a hyperlink in the Title column to view the generated report.

Sending Published Reports via E-mail

To send published reports via e-mail

- 1 Click **Scheduled** on the Actions pane.
EventTracker displays the Scheduled page.
- 2 Click the  icon in the top pane.
EventTracker displays the 'Send Report via Email' pop-up window.
- 3 Type appropriately in the From, To, CC, and Subject fields and then click **Send**.

Running Scheduled Reports On Demand

To run scheduled reports on demand

- 1 Select a report schedule in the bottom pane.
- 2 Click **Run Now**.
EventTracker displays the 'Schedule run now' pop-up window.

Table 36

Field	Description
Latest Scheduled Interval	Generate the saved report with latest scheduled interval.
Previous	Select this option to generate the report for the number of previous Day(s), Week(s) or Month(s) from the day of configuration of the selected report. The number of reports generated will depend on the Schedule option you have configured in the Report Option tab. For example, you have scheduled a daily report and have chosen to run the report for 1 month previous to the actual schedule; EventTracker will generate number of reports in proportion to the number of days in the previous month. If it's a weekly report, EventTracker will generate reports in proportion to the number of weeks in the previous month. Say for instance 30 days 30 reports and 5 weeks 5 reports respectively.
Selected Day	Select this option to run the report for the day you select from the calendar control.
Selected Month	Select this option to run the report for the selected month. The number of reports generated will depend on the number of days in the selected month.
Selected Period	Select this option to run the report for the selected period. Say for instance, if choose 7 days then EventTracker will generate 7 reports.

- 3 Select an appropriate option and then click **Generate**.
EventTracker displays the Disk Cost Analysis.

4 Cross-check the disk cost analysis and then click **Yes** to continue.

On Demand Reports

On Demand reports can be generated in the foreground and background as well. Reports that are generated in the background are called Queued reports.

On Demand page has two panes Overview and Queued.

Table 37






Field	Description
Notes	Click the  icon to add and view review notes.
Title	Name of the report. Click the title to view the report.
Created on	Date and time when the report was created.
Size(kb)	Size in KB of the report.

Table 38

Click	To
	Search published reports.
	Refresh the pane.
	Export the list of generated scheduled reports in to Excel format.
 Show all	Display all the scheduled/queued/defined report & analysis in the Reports dashboard.

QUEUED

Table 39

Field	Description
Title	Name of the report.
User name	Name of the user who has generated the report.
Start	Date and time of the configured start time.
End	Date and time of the configured end time.
Configured on	Date and time when the report was configured.
Updated on	Date and time when the report was modified.
Status	Status of the report such as New, Success, processing, Failed and No data and Cancelled.

Table 40

Field	Description
New On Demand	Configure a new report to generate in the foreground.

Field	Description
New Queued	Configure a new report to generate in the background.
Edit	Edit a report.
Delete	Delete a report.
Run now	Generate a report.

Generating On Demand Reports – Foreground

This option helps to generate On Demand in foreground.

To generate Advanced On Demand reports in the foreground

- 1 Log on to EventTracker Enterprise.
- 2 Click **Reports**.
- 3 Click Compliance / Security / Operations / My EventTracker.
- 4 Expand a reports node and right-click a report.
- 5 From the shortcut menu, choose **On Demand**.
EventTracker displays the Reports Wizard.
- 6 Click **Next >>**.
- 7 Select the Categories (when applicable), and then click **Next >>**.
- 8 Select **Sites/Systems/System Groups**.
- 9 Click **Next >>**.
- 10 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 2 Days.
- 11 Select the **Export type** as **Quick View**.
- 12 Select the **Sort by** option.
- 13 Type appropriate Refine, Filter options, and then click **Next >>**.
- 14 Type the **Title, Header, Footer, and Description**.
- 15 Click **Next >>**.
- 16 Crosscheck the Disk cost analysis details.
EventTracker disables the Publishing options.
- 17 Click **Next >>**.
- 18 Crosscheck the Report parameters.
- 19 Click **Generate Report**.

EventTracker displays the generated report in the Power Viewer.

- 20 Click **Save to file** to export and save the report on your hard disk.

EventTracker displays the '**Export Crystal**' dialog box.

- 21 Select the export type from the **Export Type** drop-down list.

- 22 Click **Yes**.

After saving the report, EventTracker displays the message box.

- 23 Click **OK**.

- 24 Click **Dashboard** in the Actions pane to view the report.

EventTracker displays the generated report and its details on the Dashboard.

Generating On Demand Reports – Foreground – Power Viewer

This option helps to generate On Demand in foreground. The generated report is displayed in the Power Viewer. With Power Viewer you can refine the result set by providing appropriate search criteria.

To generate Advanced On Demand reports in the foreground

- 1 Log on to EventTracker Enterprise.
- 2 Click **Flex Reports**
- 3 Click **Details** under Logs.
- 4 Select the **On Demand** option from the shortcut menu.
EventTracker displays the Reports Wizard.
- 5 Click **Next >>**.
- 6 Select the Category or select Custom properties.
- 7 Click **Next >>**.
- 8 Select Sites/Systems/System Groups, and then click **Next >>**.
- 9 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 2 Days.
- 10 Select the **Export type** as **Quick View**.
- 11 Select the **Sort by** option, and then click **Next >>**.
- 12 Type appropriate Refine, Filter options and then click **Next >>**.
- 13 Type the **Title**, **Header**, **Footer**, and **Description**, and then click **Next >>**.
- 14 Crosscheck the Disk cost analysis details.

EventTracker disables the Publishing options.

15 Click **Next** >>.

16 Crosscheck the Flex Reports parameters.

17 Click **Generate**.

EventTracker displays the generated report in the Power Viewer.

18 Type refine criteria to refine the result set and then click **Refine**.

19 Click **Export** to export and save the report on your hard disk.

EventTracker displays the message box.

20 Click **OK**.

EventTracker displays the generated report and report details on the Dashboard.

Generating On Demand Reports – Foreground – Smart Viewer

Smart Viewer allows you to subtly refine the intricate result set with ease. Initially Smart Viewer displays the Summary, Extended Summary and then the Detailed view. Presently supports On Demand Category based reports (Summary & Extended Summary) and Log Analysis (Summary) based on Event Categories and Custom Properties.

To generate Advanced On Demand reports in the foreground

1 Log on to EventTracker Enterprise.

2 Click **Reports**, and then click **Alphabetical reports**.

Icons C, R, and A represent Categories, Miscellaneous Reports, and Analysis respectively.

3 Select a Category. Example: *****Alerts*****.

EventTracker selects the 'On Demand' option by default.

4 Click **Next** >>.

5 Select Sites/Systems/System Groups, and then click **Next** >>.

6 Set the period for which you want the report to be generated. Example: Select the report generation interval: Last 2 Days.

7 Select the **Format option** as **Extended Summary**.

8 Select the **Export type** as **Quick View**.

9 Select the **Chart Type**.

10 Select the **Sort by** option, and then click **Next** >>.

11 Type appropriate Refine, Filter options, and then click **Next** >>.

- 12 Type the **Title**, **Header**, **Footer**, and **Description**, and then click **Next >>**.
 - 13 Crosscheck the Disk cost analysis details.
EventTracker disables the Publishing options.
 - 14 Click **Next >>**.
 - 15 Crosscheck the Flex Reports parameters.
 - 16 Click **Generate Report**.
After generating the report, EventTracker displays the Summary viewer based on the **Sort by** option you have chosen.
 - 17 Click a record to view the Extended Summary.
 - 18 Click a record in the Extended Summary to view the report in the Power Viewer.
 - 19 Click a hyperlink in the **Event Id** column to view event details in the EventTracker Knowledge Base.
-

Generating On Demand Reports – Background (Queued)

To generate Advanced On Demand reports in the background

- 1 Log on to EventTracker Enterprise.
- 2 Click **Reports**.
- 3 Click **Compliance / Security / Operations / My EventTracker**.
- 4 Expand a node and select a report type.
- 5 Click Queued / On Demand Report on the Actions pane.
- 6 Click **New Queued** in the Queued pane.
EventTracker displays the Reports Wizard.
- 7 Click **Next >>**.
- 8 Select the **Chapters** (when applicable) and then click **Next >>**.
- 9 Select the **Categories** (when applicable) and then click **Next>>**.
- 10 Select Sites/Systems/System Groups.
- 11 Set the period for which you want the report to be generated.
- 12 Select the **Format option** (when applicable).
- 13 Select an appropriate **Export type**.
- 14 Select an appropriate **Chart type** (when applicable).
- 15 Select an appropriate **Sort by** option.

- 16 Click **Next >>**.
- 17 Type appropriate **Refine, Filter** options, and then click **Next >>**.
- 18 Type the **Title, Header, Footer, and Description**.
- 19 Click **Next >>**.
- 20 Crosscheck the Disk cost analysis details.
- 21 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail.
- 22 Type valid **To E-mail** address.
- 23 Select RSS Feed from the **Update status via RSS** to receive RSS notification.
- 24 Click **Next >>**.
- 25 Crosscheck the Report parameters.
- 26 Click **Add to Queue**.

Defining Reports

Defined reports are tailor-made templates for the reports you often required to generate. Configure once and run as and when needed.

To configure Advanced defined reports

- 1 Log on to EventTracker Enterprise.
- 2 Click **Reports**.
- 3 Click **Compliance / Security / Operations / My EventTracker**.
- 4 Expand a node and select a report.
- 5 Click **Defined Reports** on the Actions pane.
(OR)
Expand a node and right-click a report.
Click **Defined** on the shortcut menu.
EventTracker displays the Defined Reports page.

Table 41

Field	Description
Title	Name of the report.
Created on	Date and the time when the template was created.
Delete	Select the checkbox and then click Delete to delete the report.

Table 42

Field	Description
New	Configure a new template.

Field	Description
Edit	Edit the template configuration settings.
Delete	Delete the selected template(s).
Schedule	Add the selected template to run as schedule report.
Add to Queue	Add the selected template to run as on demand report in the background.
Run Now	Generate the report on demand in the foreground.

- 6 Click **New**.
EventTracker displays the Reports Wizard.
- 7 Click **Next >>**.
- 8 Select the Chapters (when applicable) and then click **Next >>**.
- 9 Select the Categories (when applicable) and then click **Next>>**.
- 10 Select **Sites/Systems/System Groups**.
- 11 Set the period for which you want the report to be generated.
- 12 Select the **Format option** (when applicable).
- 13 Select an appropriate **Export type**.
- 14 Select an appropriate **Chart type** (when applicable).
- 15 Select an appropriate **Sort by** option.
- 16 Click **Next >>**.
- 17 Type appropriate **Refine, Filter** options, and then click **Next >>**.
- 18 Type the **Title, Header, Footer, and Description**.
- 19 Click **Next >>**.
- 20 Crosscheck the Report parameters.
- 21 Click **Save**.

Report Calendar

Report Calendar helps you view the time slots occupied by the scheduled reports & scheduled analyses and to use the free slots efficiently for new schedules. Exploiting the free time slots enhances the performance of reports engine, which ultimately speeds up the report generation. Report Calendar displays the time slots of the current week starting from Monday through Sunday.

To access Report Calendar

- 1 Log on to EventTracker Enterprise.

- 2 Click the **Tools** hyperlink at the upper-right corner.
 - 3 Click **Report Calendar**.
- EventTracker displays the Report Calendar in a pop-up window.

Figure 159
Report Calendar

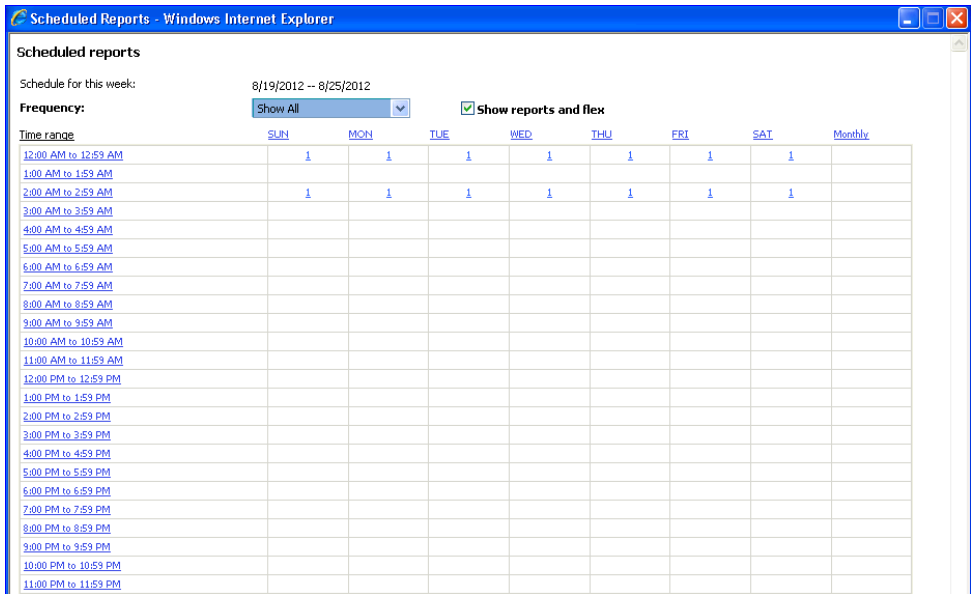


Table 43



Field	Description
Frequency	Select a frequency from this drop-down list to view respective reports.
Time range	Click to view reports / analyses scheduled in that time slot.
Day	Click to view reports / analyses scheduled on that day.
Show reports and analyses	EventTracker selects this checkbox and displays all reports and analysis schedules. Clear this checkbox and EventTracker displays only the reports schedules.


To view scheduled reports / analyses in a time slot

- 1 Click the links under **Time range**.

EventTracker displays the reports / flex scheduled in that time slot.

Table 44

Field	Description
Title	Title of the scheduled reports
Type	Type of the scheduled reports
Frequency	Frequency of the report generation
Scheduled Time	Date and time set for report generation
Configured By	Name of the user who configured the report
Comments	View read-only comments entered by the user.  indicates no comment had been entered by the user.  indicates the user had entered comments.

- 2 Click  in the Comments column.
EventTracker displays read-only Schedule Comments.

To view scheduled reports on a day

- Click the name of the day.
EventTracker displays the reports scheduled on that day.

To view scheduled reports on a particular day and a time slot

- Click the links at the intersection of Time range and Day.
EventTracker displays the reports scheduled on that day and time slot.

Report Status Snapshot

Report snapshot displays the Overview and Queue status of the reports and flex irrespective of the Collection Point Site.

- Log on to EventTracker Enterprise.
- Click the **Tools** hyperlink at the upper-right corner.
- Click the **Report Status** hyperlink.
EventTracker displays the Report Status Snapshot pop-up window.

Table 45

Field	Description
Active Users	No of user logged on to EventTracker.
User	Select a user from this drop-down list to view the count of all reports / analyses configured by that user. EventTracker populates this drop-down list only when the logged

Field	Description
	in user has Admin privilege.

Table 46

Field	Description
Title	Name of the report / flex report
User name	Name of the user who configured the report / flex report
Queue type	Says whether report is Queued or On Demand.
Duration from	Report generation interval start time. EventTracker considers events occurred at this time onwards.
Duration to	Report generation interval end time. EventTracker considers events occurred till this time.
Status	Indicates the report / f generation stages.
Last update	Date and time when the report generation was initiated.
Estimated time	Approximate time require to generate the report / flex report
Cancel processing	Click to abort report generation.

Favorites

Favorites are bookmarks to often generated on demand Reports. A Report/Category/Chapter can be added to Favorites. You can also add Flex Report to favorites list.

Adding to Favorites

To add to favorites list

- 1 Click **Reports**.
- 2 Click **Compliance / Security / Operations / My EventTracker**.
- 3 Right-click a report.
- 4 Click **Add to favorites** on the shortcut menu.
EventTracker adds the report type to the favorites list.

Viewing the Favorites list

To view favorites list

- 1 Click **Tools** dropdown, and then click the **Favorites** hyperlink.
EventTracker displays the 'Favorites List' pop-up window.

- 2 Select a report and then click **Generate Report** to generate on demand report.
-

Chapter 6

Analyzing Netflow Data

In this chapter, you will learn how to:

- [Enable EventTracker Netflow Receiver](#)
- [Interpret Netflow Data](#)

What is Netflow?

A Cisco-proprietary IP statistics collection feature that collects information on IP flows passing through a router.

Source:

<https://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qgloss.html>

For more information, click

http://www.cisco.com/en/US/tech/tk812/tsd_technology_support_protocol_home.html

Terminology

Table 47

Term	Description
Differentiated Services Code Point (DSCP)	<p>Differentiated Services (DiffServ) is a new model in which traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field.</p> <p>The six most significant bits of the DiffServ field is called as the DSCP.</p> <p>Source: http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml#dscpan_dassuredforwardingclasses </p>
Input logical interface (ifIndex)	<p>One of the first things to learn, when you are dealing with SNMP, is ifIndex. This is a primary key of all objects. Consider it a way that all of the interfaces (physical and logical) are broken down and assigned a value. This value is assigned during boot up of a device, and it may not be changed. If any information needs to be polled for that particular interface, it must use that assigned value.</p> <p>Source: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080157626.shtml </p>

EventTracker Netflow Analyzer

EventTracker Netflow Analyzer is a Netflow collector, analyzer, and reporting engine integrated together. 'EventTracker Netflow Analyzer' helps you gain in-depth visibility into your network traffic and its patterns, thus empowering you to investigate, troubleshoot, and quickly remediate network slowdowns.

- Monitor network traffic per interface
 - Configure Netflow Collector with minimal effort Visualize near real-time network traffic
 - Break-up summary with visual charts to quickly and easily identify top talkers, applications, and protocols hogging network bandwidth
 - Network traffic reports with just a few clicks
 - Long-term retention of Netflow data for trending and capacity planning
 - Cost effective
-

How it benefits you

1 Identify what applications comprises the network traffic

- a. Analyze statistics about every single application routed through the network interface
- b. Compare application usage patterns
- c. Determine potential root causes of network performance problems
- d. Prioritize applications based on ToS (Type of service).

2 Identify top conservationists

- a. Identify hosts (clients, servers, networked devices, and so on) conversed using applications
- b. Isolate top talkers that impact business-critical applications

3 Gain visibility across ports

4 Understand bandwidth utilization and growth.

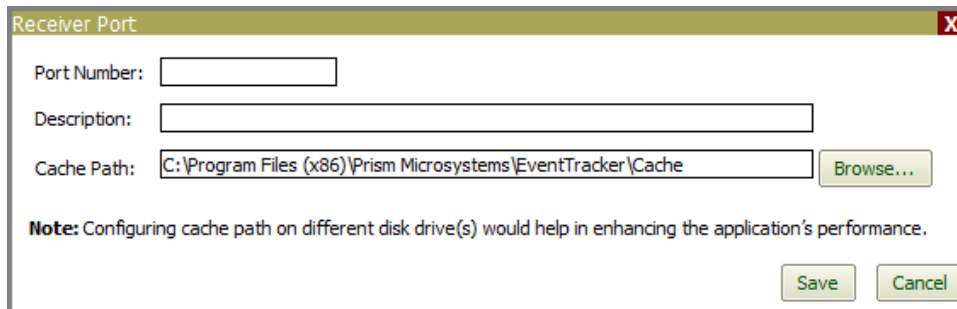
- a. Understand how bandwidth and application utilization grows over time
 - b. Plan for future capacity requirements
 - c. Make informed decisions regarding bandwidth upgrades by trending application growth on particular interfaces
-

Enabling EventTracker Netflow Receiver

This option helps to enable 'EventTracker Netflow Receiver' to collect Netflow logs.

To enable EventTracker Netflow Receiver

- 1 Log on to **EventTracker Enterprise**.
- 2 Click **Admin** dropdown, and then click **Manager**.
- 3 Click the **syslog / Virtual Collection Point** tab.
- 4 In Virtual 'Collection Points' pane, click **Add**.
EventTracker displays the **Receiver Port** pop-up window.



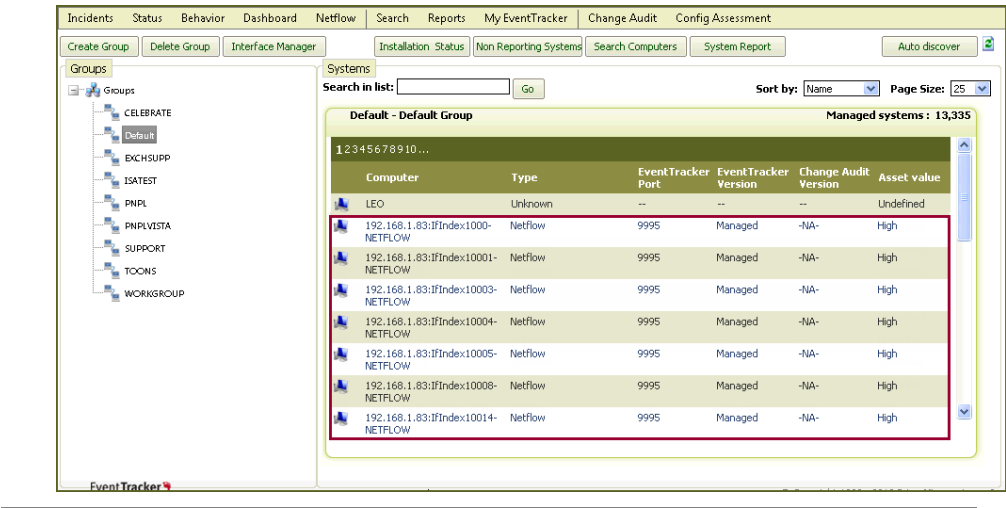
- 5 Add appropriate port details, and then click **Save**.

NOTE

This port must be exclusive to the Direct Log Archiver to archive Netflow logs.

- 6 Click the **Direct Log Archiver / Netflow Receiver** tab.
- 7 Check the **Direct log file archiving from external sources** option.
- 8 From the **Associated virtual collection point** drop-down list, select the port that you have added earlier.
Example: Port number 9995
- 9 In the **Netflow data storage folder** field, type the path of the folder where Netflow logs are dumped.
(OR)
Click the **Browse** button to select the folder.
You can use the default ports or add ports to collect Netflow logs. Default netflow data storage folder can be used for the newly added ports.
- 10 Click **Save**.
To collect Netflow data, EventTracker creates a netflow system instance once you enable netflow receiver.

Figure 160
Netflow system
instance



Interpreting Netflow Data

This option helps to view and interpret Netflow logs collected by EventTracker Netflow Receiver.

To interpret Netflow logs

- 1 Click the **Netflow** menu.

EventTracker displays the **Conversations** tab on the Netflow Dashboard, provides historical trends conversations happened between network interfaces.

Figure 161
Conversations tab

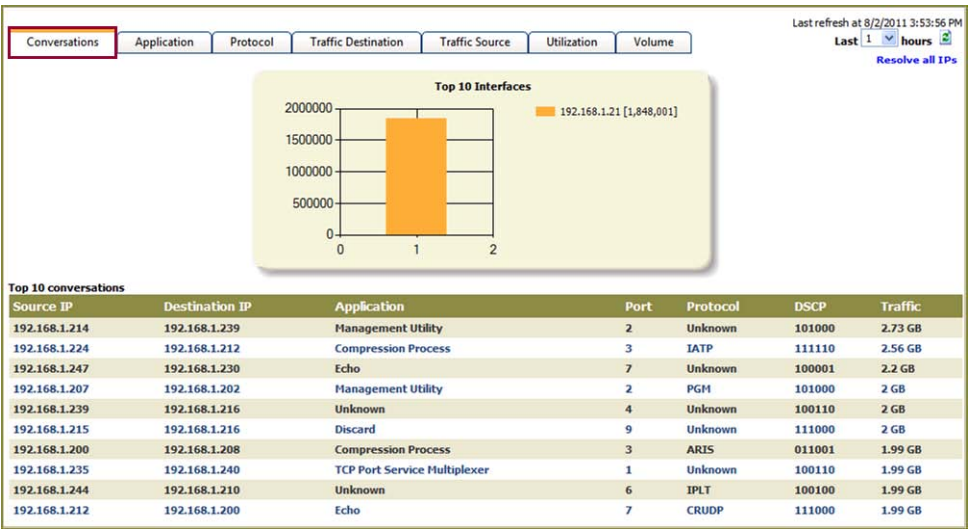


Table 48

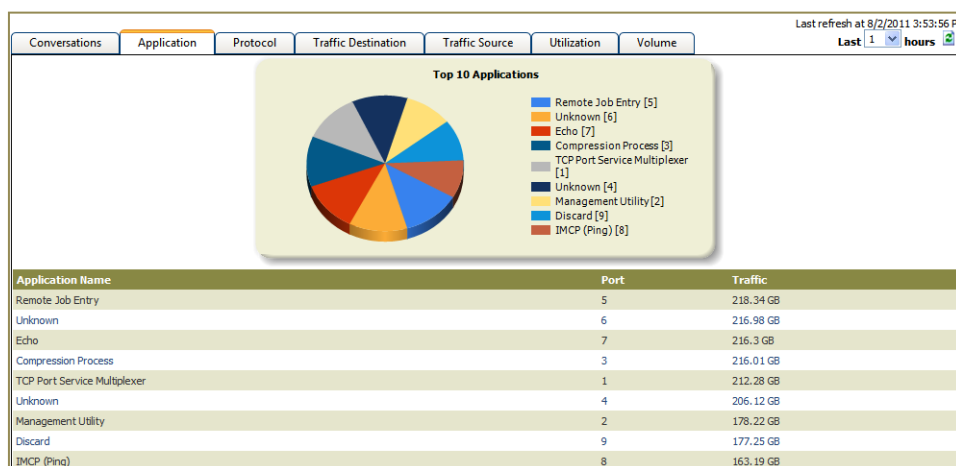
Term	Description
Source IP	Interface IP from where the conversation originated.

Term	Description
Destination IP	Interface IP to where the conversation is destined for.
Application	Application that was used.
Port	Port through which the communication happened.
Protocol	Protocol that was used to carry on the conversation.
DSCP (Differentiated Services Code Points)	DSCP is a 6 bit value. The six-bits of the DS field are used as a codepoint to select the PHB (Per Hop Behavior) a packet experiences at each node.
Traffic	Aggregation of bytes between the source and destination during a specified period of time.

2 Click the **Application** tab.

Provides historical trends of applications used.

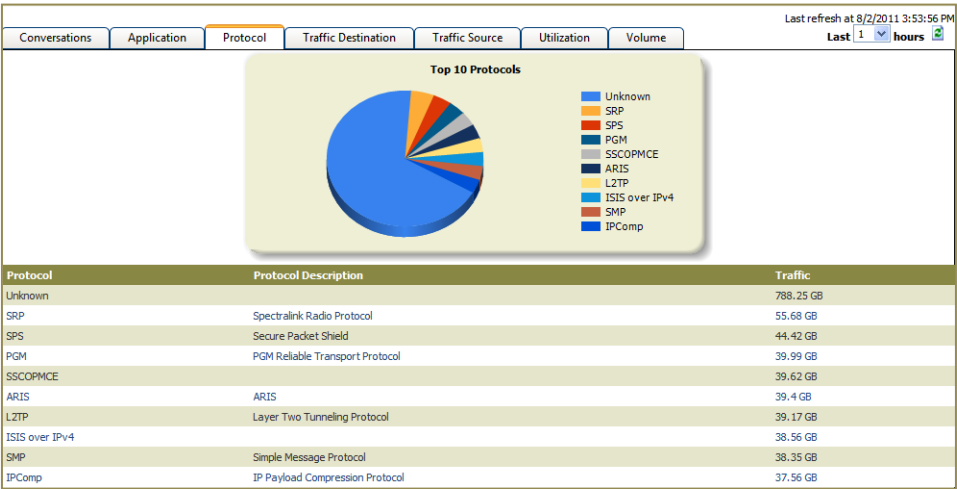
Figure 162
Application



3 Click the **Protocol** tab.

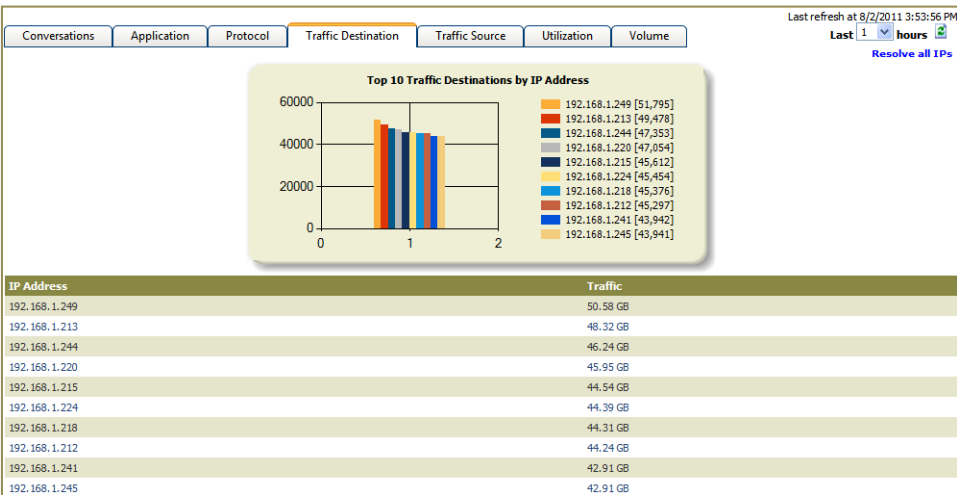
Provides historical trends of protocols used.

Figure 163
Protocol



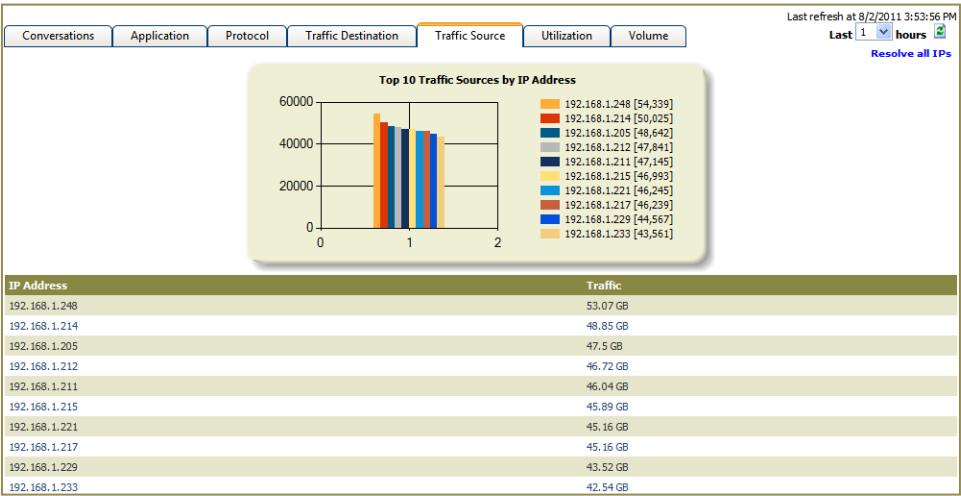
- 4 Click the **Traffic Destination** tab.
Provides historical trends of destination to where the traffic destined for.

Figure 164
Traffic Source



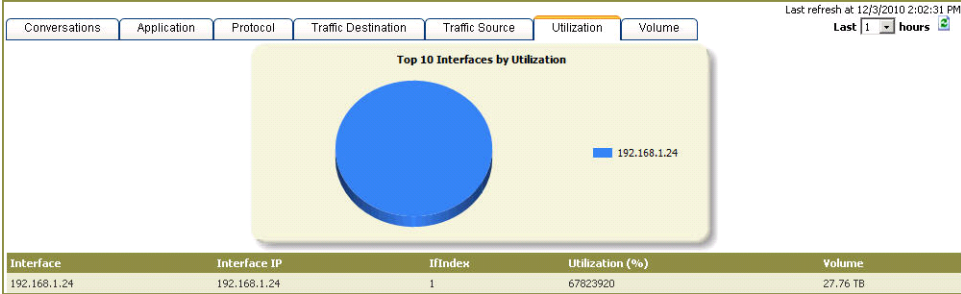
- 5 Click the **Traffic Source** tab.
Provides historical trends of source from where the network traffic originated.

Figure 165
Traffic Source



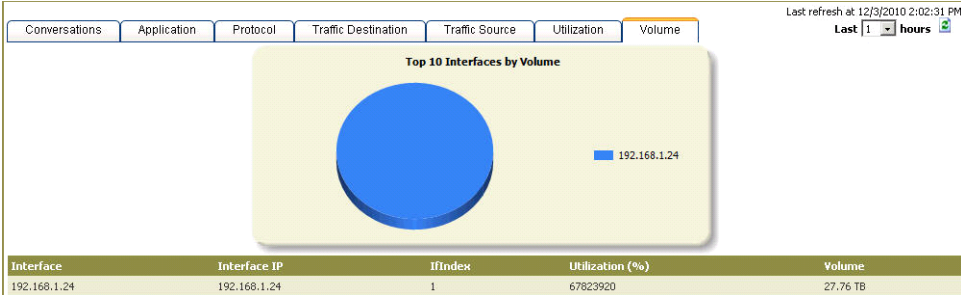
- 6 Click the **Utilization** tab.
Provides historical trends of utilization of network interfaces.

Figure 166
Utilization



- 7 Click the **Volume** tab.
Provides historical trends of volume of traffic that happened through network interfaces.

Figure 167
Volume



Interface Manager

This option helps to modify the interface details.

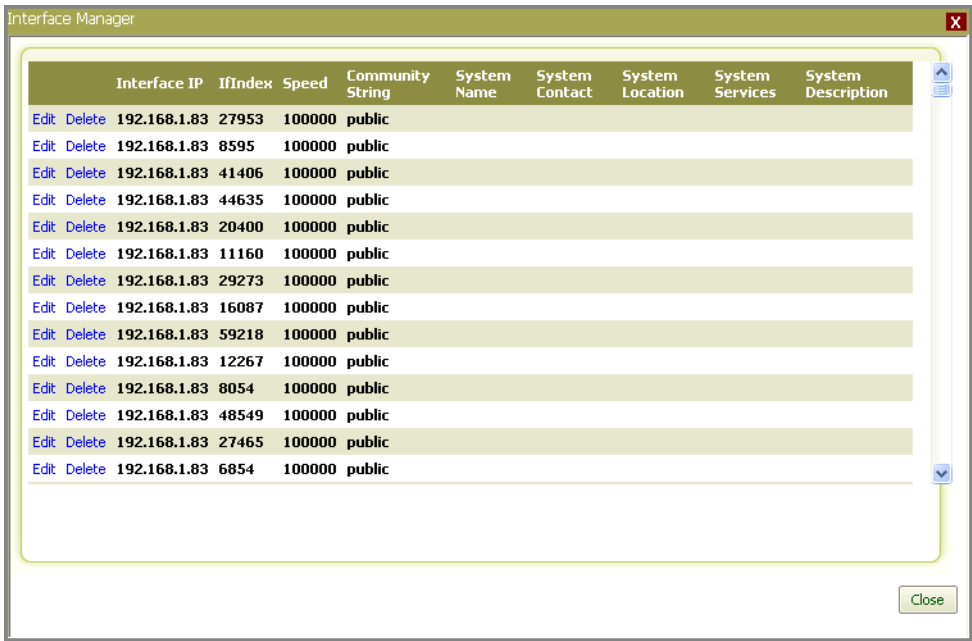
To modify interface details

- 1 Click **Admin** dropdown, and then select **Systems**.
- 2 In the 'System Manager' page, click the **Interface Manager** button.

EventTracker displays the Interface Manager dialog box.

Figure 168
Interface Manager

Interface manager displays the list of devices that collect IP traffic statistics on all the interfaces where Netflow is enabled.

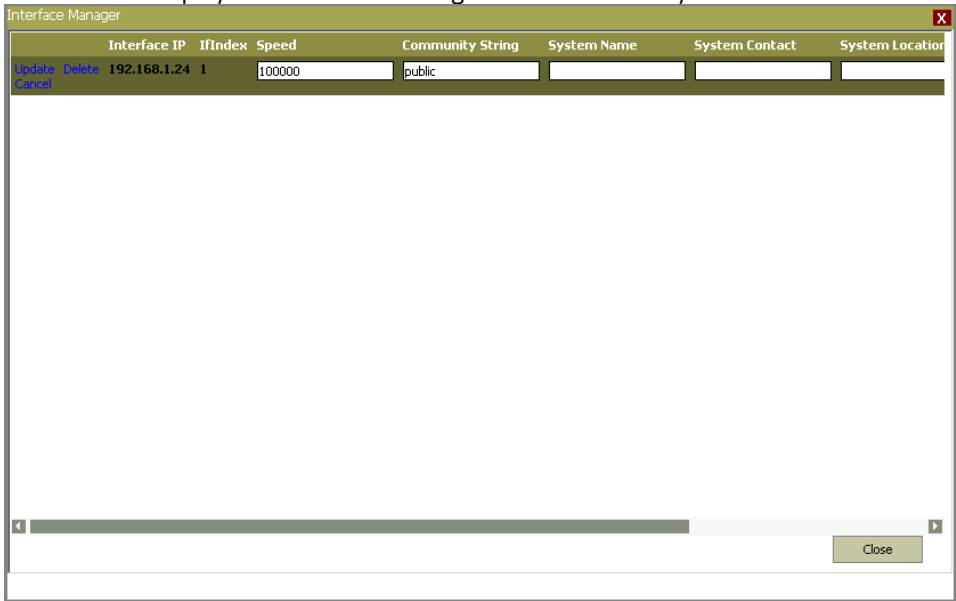


- 3 Click **Edit** to modify details.

EventTracker displays the Interface Manager window to modify details.

Figure 169
Interface Manager

Interface manager displays the list of IP addresses and various system parameters that were configured during the packet transmission.



- 4 Type appropriately in the relevant fields.

5 Click **Update**.

EventTracker updates the changes made.

(OR)

Click **Delete** to delete the Interface Manager details.

EventTracker displays the confirmation message box.

Chapter 7

Viewing Windows System Status

In this chapter, you will learn how to:


- [View Windows System Status](#)

Viewing Managed Windows System Status

In the EventTracker, you can get a peek view of the Windows system status.

Table 49

Tab	Click to
TABS	
System Details	View system details like O/S type, Asset value and top 10 Alert events occurred in the last one-hour. At the maximum you can opt to view alert events occurred in the last 24 hours. Click the refresh button to refresh the pane with recent alert details.
Event Category	This report provides per Category count of *All error events, *All information events, *All warning events, *All audit success events, *All audit failure events occurred in the last one-hour. At the maximum you can opt to view events occurred in the last 24 hours. Click the refresh button to refresh the pane with recent events.
Event Source	This report provides per source event count. Helps to identify top 10 event sources for the last one-hour. At the maximum you can opt to view sources for the last 24 hours. Click the refresh button to refresh the pane with recent source of events.
File/Resource Access Failures	<p>Failed attempts to access shared resources such as files and folders are captured by these reports. Windows file/folder auditing must be enabled appropriately for these reports to generate meaningful data.</p> <p>Usage: These reports are usually run and reviewed regularly to detect access to mission critical resources.</p>
Login Failures	The security logon features include logging all unsuccessful login attempts. The user name, date and time are included in this report.
Log Volume	<p>Provides information on count of events received from the selected system.</p> <p>Usage: This report can be used to analyze maximum occurring events.</p>
Patches / Hot Fixes	View details on patches / hot fixes applied on the server.
Printer Activity	<p>View information on printer utilization providing details on jobs, users and pages sorted by print servers or users.</p> <p>Usage: This report can be used for chargeback of printer usage or from a security perspective to note unusual printer activity.</p>
Software Installed	The EventTracker Agent for Windows can be configured to detect the installation of software applications. If this feature is enabled, this report provides information on software application install on the EventTracker Server for the chosen

Tab	Click to
	time period. Usage: This report is useful to track updates or changes to critical systems.
Software Usage	The EventTracker Agent for Windows, can be configured to detect the start and stop of software applications. If this feature is enabled, this report provides information on software application utilization across selected computers for the chosen time period. Usage: This report is typically used to manage licensing or to determine usage of specific applications. It is more useful on Workstations than on Servers
Storage	Disk utilization is a critical resource for servers and must be monitored. This report helps identify disk space availability and the presence of bad blocks. Usage: This report is used to decide on preventive remedial measures so as to minimize downtime or declining service levels.
Suspicious Network Activity	The classic virus infection causes unrecognized EXEs to begin accessing the network. When enabled, the EventTracker Agent for Windows can be configured with a white-list of known ports or application and report exceptions. This helps identify potentially suspicious traffic. The report uses a database of known infections per port to identify potential threats. Usage: After suitably configuring the EventTracker Agent for Windows, this report is used to report on unusual traffic from unrecognized EXEs.
USB File Activity	This report provides per user details on USB activities that include file addition, deletion, changes, and respective total no. of times those activities were done.
	Refresh the Dashboard.
Last hours	Select the time interval you wish to generate report.

To view Windows system status

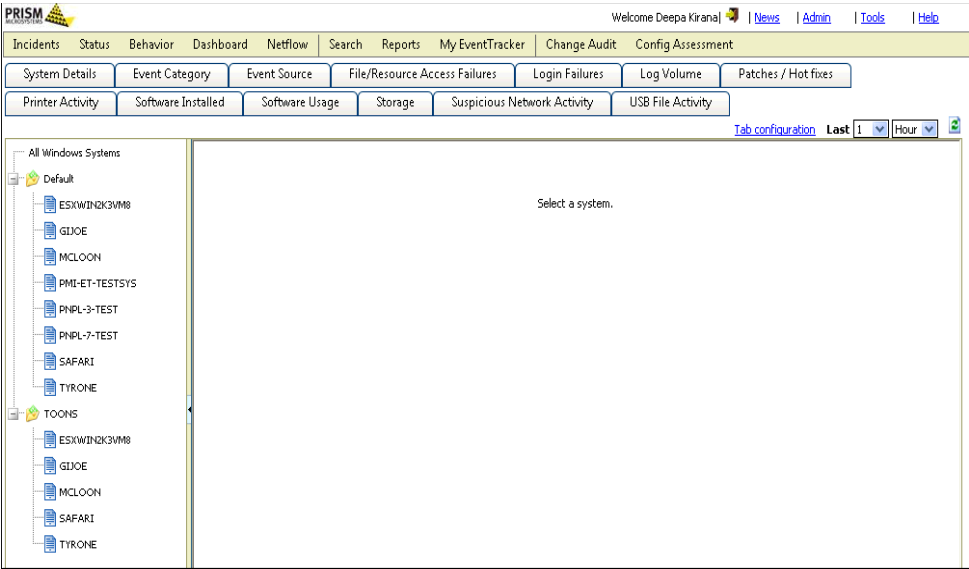
This option helps to quick view status of the managed Windows systems.

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Tools** dropdown, and then click **Windows**.
EventTracker displays the 'Windows Systems Dashboard'.

NOTE

EventTracker displays only the managed system groups systems and DLA system instances on the left pane.

Figure 170
Windows systems



- 3 Right-click a system on the left pane and then click **Show Details**.
EventTracker displays the **System Details** tab and the relevant details.
- 4 Click a tab to view summary report.
You can also select multiple tabs for parallel processing.
- 5 If displayed, click the **Detail** button to view detailed report.
EventTracker displays the File Download pop-up window.
- 6 Click **Save** to save the *.pdf file in a safer location for future reference.

Loading Tabs Together

This option helps you select tabs that you wish to load together, that is to process concurrently instead of selecting individual tabs.

To load tabs together

- 1 Click the **Tab configuration** hyperlink.
EventTracker displays Tab configuration window.

Figure 171
Load together
configuration

Had you selected a tab and then configured tabs, EventTracker still focuses on the current tab and starts processing the other tabs you have configured in the background.

Advantage of configuring tabs is that processing continues in the background even if you select other tabs.



- 2 Select the **Tab name** option(s) that you wish to load together, and then click **Save**.
- 3 In All Windows Systems pane, right-click system name, and then click **Show Details**.

EventTracker turns focus on the **System Details** tab and displays the relevant details. Also starts processing concurrently in the background the other tabs you have configured.

You can also select tabs other than tabs you have configured to load together.

EventTracker starts processing only when a tab is selected. When you click a new tab and come back to the previous tab, EventTracker starts processing afresh.

 **NOTE**

You have to select at least two tabs on the **Tab configuration** window. EventTracker displays the message box with appropriate message if you select just one tab.

Chapter 8

Viewing Logs

In this chapter, you will learn how to:

- [View Logsc](#)

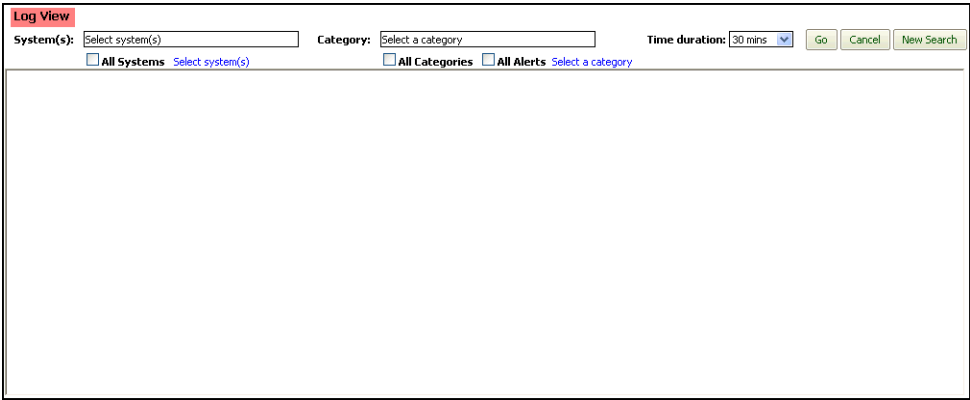
Viewing Logs

This option enables you to view category wise events occurred at managed systems.

To view logs

- 1 Log on to EventTracker Enterprise.
- 2 Click the **Tools** dropdown, and then click **Log View**.

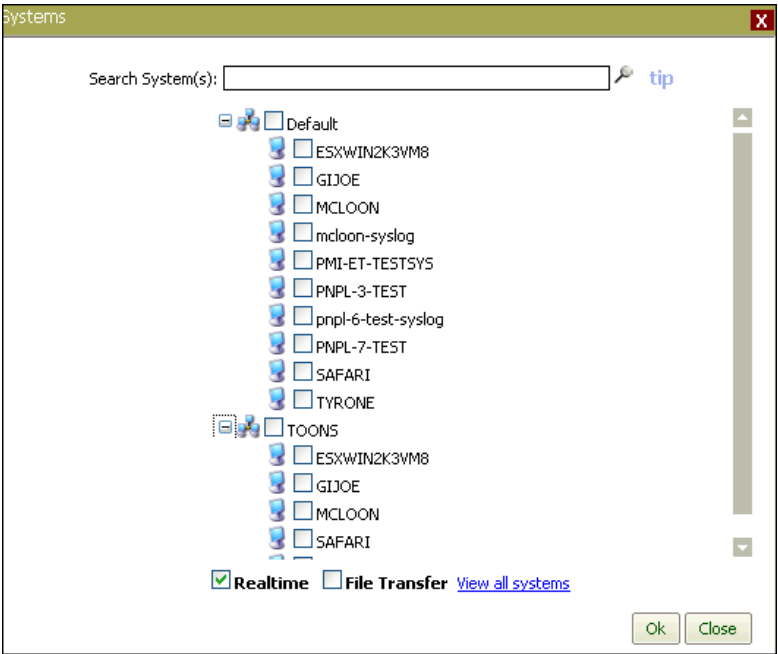
Figure 172
Log View



- 3 Check the **All Systems** option to view logs of all managed systems (OR) click the **Select system(s)** hyperlink to make customize selection.

EventTracker displays **Systems** pop-up window.

Figure 173
Systems



Enter the system name in **Search system(s)** field or select a group/system(s), and then click **Ok**.

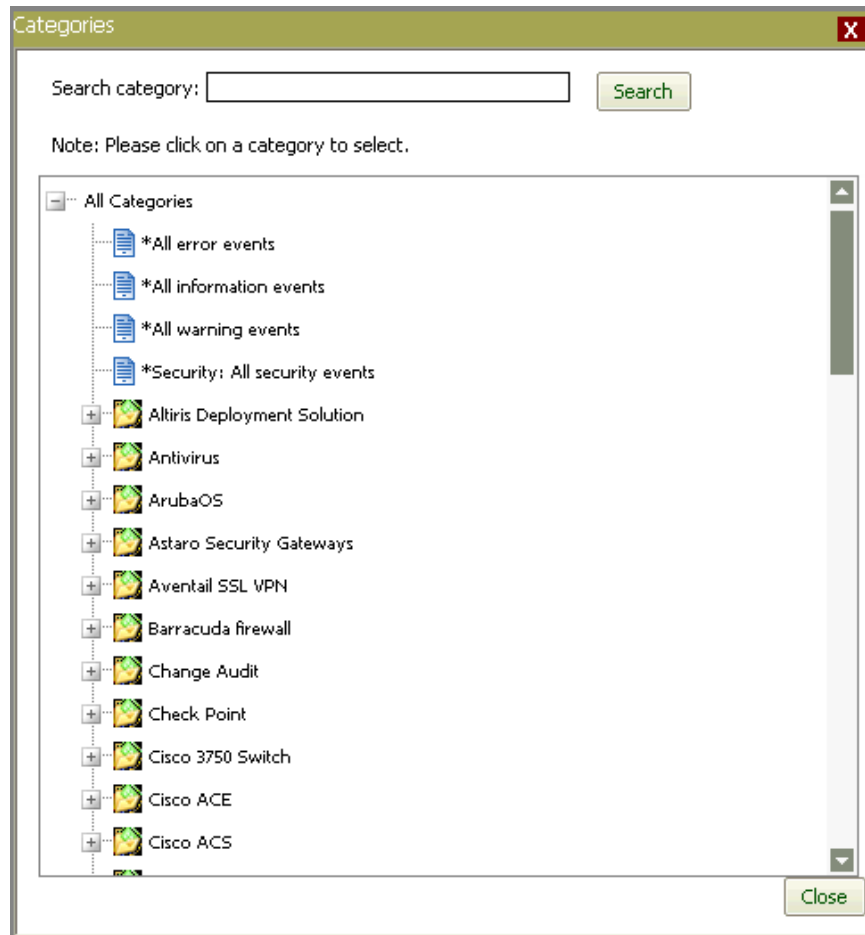
- 4 Check the **All Categories** option to view all category events (or) check the **All Alerts** option to view all alert events.

(OR)

Click the **Select a category** hyperlink.

EventTracker displays **Categories** pop-up window.

Figure 174
Categories

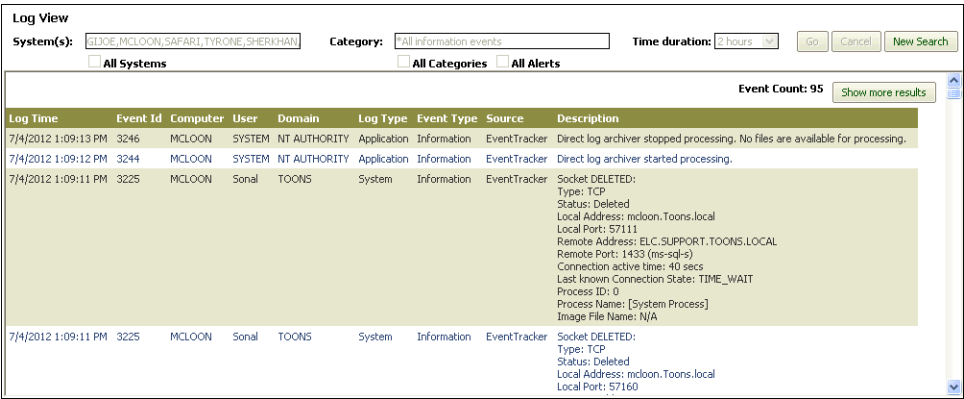


Enter category name in the **Search category** field (or) click category name in the category tree, and then click **Close**.

- 5 Select the period from **Time Duration** drop-down list.
- 6 Click the **Go** button.

EventTracker displays the search result.

Figure 175
Log View



- 7 Click **Show more result** button, to see more results on the given search criteria.
- 8 Click **New Search** button to clear the search criteria and start afresh search.

NOTE

From **Log View**, an event can be added as an alert.

In the Event ID column, click the event Id dropdown, and then click **Add as Alert**. EventTracker displays 'Alert Configuration' window. Make the required changes, and then click the **Finish** button.

Chapter 9

Configuring Manager

In this chapter, you will learn how to:

- [Enable Alert Notification Status Tracking](#)
- [Purge Alert Events Cache](#)
- [Configure Config Assessment Settings](#)

Configuration- Alert Events

Alert Events

☒ Enable alert notification status

☒ Enable alert events cache for analyzing alerts

Purge events from cache older than days

☐ Turn off alerts

☐ Turn off filters

☒ Enable remedial action

☐ Suppress duplicate alerts

Alert suppression interval: seconds

Maximum number of alerts allowed:

Enabling Alert Notification Status Tracking

This option helps you track success/failure alert notification status.

To enable alert notification status tracking

- 1 Click the **Admin** dropdown, and then click **Manager**.
- 2 Click the **Configuration** tab, if not selected.
- 3 Select the **Enable alert notification status** checkbox, if not selected by default.

NOTE

You might receive notifications for the configured alerts, but you may not be able to track the success/failure status of those notifications if you disable this option.

- 4 Click **Save**.

Purging Alert Events Cache

This option helps you purge alert events cache. By default, EventTracker retains event data for seven days. You can configure to hold minimum 24-hour and maximum 90 days event data. You cannot completely purge the cache.

To purge Alert Events Cache

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
- 2 Select the **Enable Alert Events Cache for Alert Analysis** checkbox, if not selected by default.

EventTracker enable **Purge events from cache older than – days** field, if not selected by default.
- 3 Type the duration in **Purge events from cache older than – days** field.
- 4 Click **Save**.

Enabling Remedial Actions

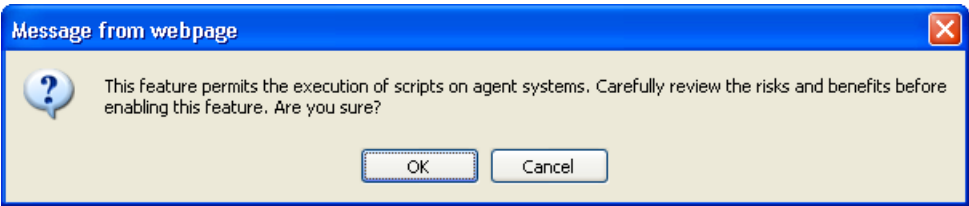
It is mandatory to enable remedial action at the manager console. Otherwise, you cannot execute remedial action at the agent systems.

To configure remedial action

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
- 2 Select the **Enable Remedial Action** checkbox, if not selected by default.

EventTracker displays the Caution dialog box.

Figure 176
Remedial Action
Configuration



- 3 Click **OK**.
- 4 Click **Save**.

Suppressing Duplicate Alerts

WHAT DOES "DUPLICATE ALERT SUPPRESSION" MEAN?

EventTracker provides the facility of generating user configurable alerts for events received by the EventTracker. This feature is very useful in case the user is not always available at the manager console.

In case the multiple instances of an event with a configured alert are received in a short period of time then a large number of alerts will be generated, this could confuse the user.

'Duplicate Alert Suppression' feature will handle such a deluge of alerts by suppressing any alert in case it is a duplicate of an alert received earlier, within a particular time frame.

Sample Alert Suppression setting:

Figure 177

The above settings inform the EventTracker to allow a MAXIMUM of 5 DUPLICATE alerts to be triggered within a timeframe of 300 seconds. An alert is considered a duplicate only if it is triggered by the same event.

This option helps you suppress duplicate alerts.

To suppress duplicate Alerts

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
 - 2 Select the **Suppress Duplicate Alerts** checkbox.
EventTracker enables the **Alert suppression interval** and **Maximum number of alerts allowed** fields.
 - 3 Type appropriately in the relevant fields.
 - 4 Click **Save**.
-

Configuration- Correlation Receiver

This option helps you configure correlation receiver port to receive results of correlation rules.

By default, correlation receiver receives rules through port 14509.

To configure correlation receiver port

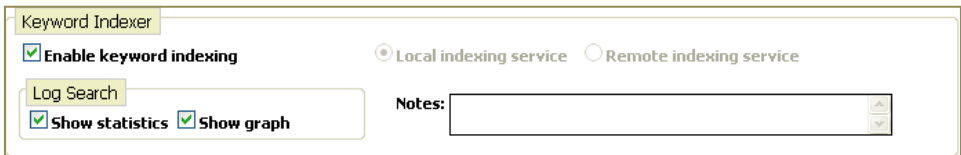
- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
- 2 Type the port number in the **Send results of all correlation rules to port** field.
- 3 Click **Save**.

Note

If 'Event Correlator' is not installed, then 'Correlation Receiver' pane is grayed out/ disabled.

Configuration- Keyword Indexer

EventTracker by default selects **Show statistics** and **Show graph** options in the **Log search** pane.



Enabling Keyword Indexing

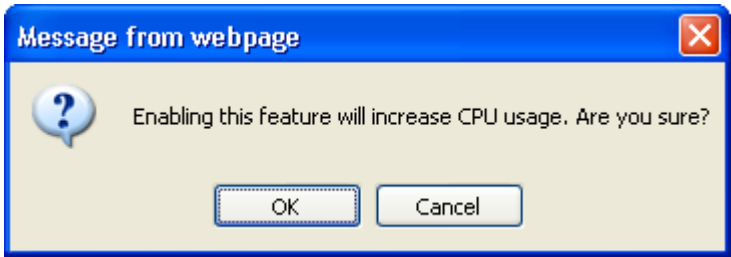
This option helps you enable the 'Keyword Indexer' service to index keywords.

To enable keyword indexing

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
- 2 Select the **Enable Keyword Indexing** checkbox.

EventTracker displays caution dialog box.

Figure 178



3 Click **OK** to continue.

Table 50

Field	Description
Local Indexing service	Keyword indexing process is carried out on the local machine. You are not allowed to change this option.
Remote Indexing service	Keyword indexing process is carried out on a remote machine to reduce the resource utilizations of the manager. You are not allowed to change this option. Click here for more information on Remote Indexing.
Show statistic	Show/hide the statistics in the log search page. Clear the Show statistic checkbox to view only graphs in the log search page.
Show graph	Show/hide the graphs in the log search page. Clear the Show graph checkbox to view only statistics in the log search page.

4 Click **Save**.

NOTE

Show statistics and **Show graph** option is not enabled after upgradation.

'Keyword Indexing' option is enabled by default on fresh install and will be grayed out in case the 'Keyword Indexing' feature is not present in the certificate file.

Clear the **Enable Keyword Indexing** checkbox if the 'Keyword Indexer' hogs the system resources.

Configuration- EventTracker Knowledge Base Web Site



Configuration

KB website :

☒ Check for knowledge base updates

This option enables you to configure 'EventTracker Knowledge Base' Web site.

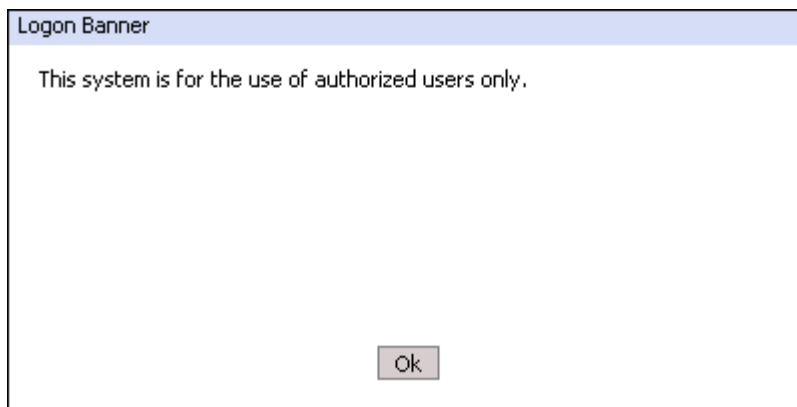
To configure EventTracker Knowledge Base Web site

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
- 2 Type the URL of the Knowledge Base Web site in the **KB Website** field.
- 3 Check the **Check for knowledge base updates** option, if unchecked.
- 4 Click **Save**.

Configuration- Logon Banner

This option helps you configure the custom log on message. This banner is displayed to anyone who tries to gain access to EventTracker, prior to typing the user credentials. This could be a warning message or a custom message such as 'Welcome! User' or 'This system is for the use of authorized users only.'

Figure 179
Log on Banner



Logon Banner

This system is for the use of authorized users only.

Ok

To configure custom Log on message

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
- 2 Type the warning or custom message in the **Logon Banner** field.
- 3 Click **Save**.

Configuration- Cost Savings

Enable 'Collecting Cost Savings Information' option to run ROI reports (**Reports** -> **Flex Reports** -> **Cost Savings**). Enabling this option might hit the performance of 'EventTracker Archiver' process if the load of events to be processed is heavy.

To enable Collecting Cost Savings Information

- 1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
 - 2 Check the **Collect Cost Savings Information** option.
 - 3 Click **Save**.
-

Syslog / Virtual Collection Point

EventTracker by default selects the 'Enable syslog receiver' option to enable the EventTracker receiver to receive syslogs sent by non-Windows systems.

To enable syslog receiver

- 1 In **Manager Configuration** page, click the **syslog / Virtual Collection Point** tab.
 - 2 Select the **Enable syslog receiver** checkbox, if not selected by default.
 - 3 Click **Save**.
-

Monitoring syslogs

For monitoring syslog events, you must configure the UNIX computer to forward syslog events to the computer where the EventTracker Manager is installed. The default syslog port is UDP Port=514. Also, see the FAQ on syslog.

To configure UNIX systems to forward syslog messages to EventTracker

- 1 Identify the IP Address of the computer that is hosting the EventTracker Manager.
- 2 Log on with the root account in the UNIX computer.
- 3 Open the [syslog.conf](#) file in a text editor. The default path of the syslog.conf file is [/etc/syslog.conf](#).
- 4 Append the configuration details in the [syslog.conf](#) file to forward syslog messages to the EventTracker Manager computer.
- 5 Save and close the [syslog.conf](#) file.
- 6 Stop and restart the syslog daemon (syslogd).

Example: To forward syslog error messages to the IP address 192.192.150.150, add the following detail to the syslog.conf file. *.err @192.192.150.150

NOTE

For more information, refer the [syslog.conf](#) or syslog MAN pages.

Syslog configuration may be platform-dependent and it is recommended that you check the platform documentation.

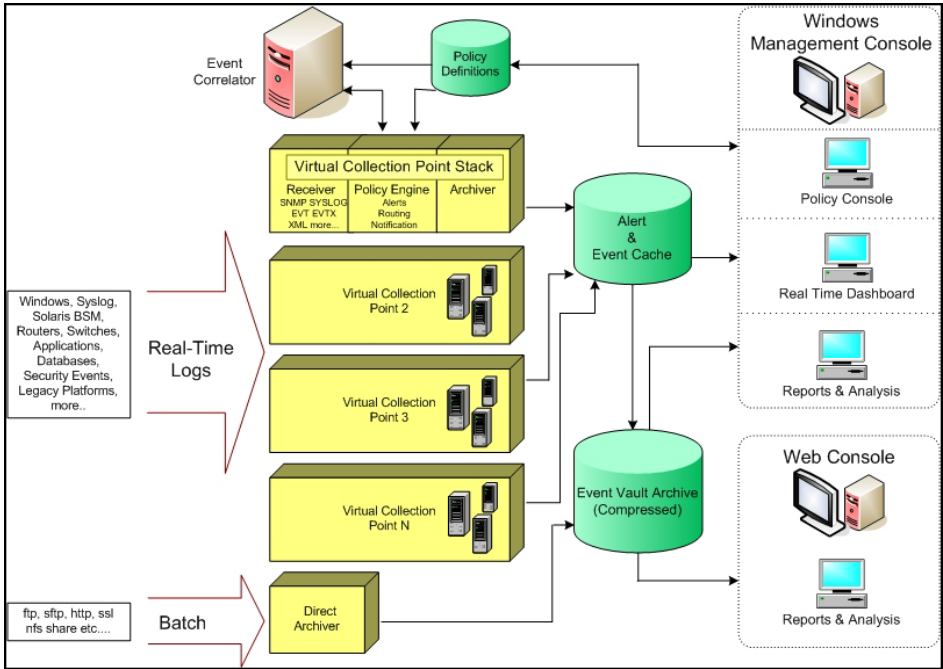
Virtual Collection Points

Virtual Collection Points (VCP) enable the existing receiver to behave like a collection master without having the physical Collection Points installed. The Existing Collection Point (CP-CM model) requires physically organized Collection Points reporting to a Collection Master. CP-CM model requires a number of hardware facilities and a large degree of deployment difficulty.

VCP provides the solution to break down the huge volume of input events using the existing set up with minimal configuration changes, thus helps to process the received data in a short time at the reporting end.

VCP ARCHITECTURE

Figure 180
VCP Architecture



Configuring EventTracker Receiver to Listen on Multiple Ports

EventTracker Receiver can be configured to listen any number of ports for Traps and Unix/Linux/Solaris syslogs.

The internal limit for number of VCP's (which was 10 Windows & 10 SYSLOG) has been removed. Now, based on the system capacity (Disk, RAM, CPU, etc) any number of VCP's can be added.

Table 51

ET Modules	Suggested Trap Ports
You need to add the ports that you are using to the Firewall exceptions list.	
EventTracker Receiver (Incoming)	14505 default port. 14515, 14525, 14535, 14545, 14555, 14565, 14575, 14585, 14595 514 (UDP/TCP) for syslogs.

For more information, refer [EventTracker v7.0 Enterprise VCP.pdf](#)

Virtual Collection Points for syslogs

Configuring EventTracker Receiver Ports

This option helps you configure EventTracker receiver to listen on different ports.

To configure virtual collection points for syslogs

- 1 Click the **syslog / Virtual Collection Point** tab.
- 2 Check **Enable syslog receiver** option if not checked by default, and then click **Add**.

EventTracker displays the **Syslog Receiver Port** dialog box.

Figure 181
Syslog Receiver Port

- 3 Type appropriate **Port Number** and **Description** in the respective fields.
- 4 In the **Cache path** field, type/ browse the path to save the cache files.
This is not mandatory, but changing the location would result in enhancing application's performance.
- 5 Click **Save**.

Forwarding Raw syslog Messages

This option helps you forward received syslog messages in raw format i.e. forwarded with the same format as it is received to a specified destination.

To forward syslog messages in raw format

- 1 Select the **Raw syslog Forward** checkbox.
- 2 Type the host name or IP address of the destination in the **Trap Destination** field.
- 3 Select an appropriate **Mode** of transport.
- 4 Type an appropriate port with respect to the mode chosen.
- 5 Click **Save**.

Virtual Collection Points for Windows Events

EventTracker Receiver can be configured to listen on 10 ports for Windows Events.

Example Scenario

Consider EventTracker Agents in computers Sys2 and Sys3 are forwarding events to Sys1 (EventTracker Manager). By default, the communication happens through port

14505. Suppose you want to configure different ports say for example 14515 and 14525 for Sys2 and Sys3 respectively, do the following:

Computer: Sys1 – Configuring Ports

- 1 In **syslog / Virtual Collection Point** tab, click **Add** button under **Virtual Collection Points** pane.

EventTracker displays the **Receiver Port** dialog box.

Figure 182
Receiver Port

Receiver Port

Port Number:

Description:

Cache Path:

Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.

- 2 Type appropriate **Port Number** and **Description** in the respective fields.
- 3 In the **Cache path** field, type/ browse the path to save the cache files.
- 4 Click **Save**.

EventTracker adds the newly configured ports.

EventTracker updates these changes in `evtrxr.ini` file (`...\Program Files\Prism Microsystems\EventTracker`)

EventTracker creates `EtaConfig_14515.ini` & `EtaConfig_14525.ini` files in RemoteInstaller folder

(`...\ProgramFiles\Prism Microsystems\EventTracker\RemoteInstaller`).

Table 52

EventTracker Modules	Trap Ports utilized
You need to add these ports to the Firewall exceptions list	
EventTracker Receiver (Incoming)	14505, 14515, 14525

Upgrading Agent (Sys2) from Manager (Sys1)

- 1 Click the **Admin** dropdown, and then click **Systems**.
- 2 Move the pointer over the system (sys2) that you wish to upgrade, and then click the dropdown.
- 3 From the shortcut menu, select **Upgrade agent**.
- 4 Select an appropriate agent to upgrade, and then click **Next**.
- 5 Click **Advanced**.

- 6 Select **Custom config** option.
- 7 Select the path of the custom ini file ([EtaConfig_14515.ini](#)) from the **File** dropdown.
- 8 Click **Upgrade**.
EventTracker overwrites [etaconfig.ini](#) file with new settings.

Upgrading Agent (Sys3) from Manager (Sys1)

- 1 Open the **System** Manager.
 - 2 Click the system (sys3) that you wish to upgrade.
 - 3 From the shortcut menu, select **Upgrade agent**.
 - 4 Select an appropriate agent to upgrade, and then click **Next**.
 - 5 Click **Advanced**.
 - 6 Select **Custom config** option.
 - 7 Select the path of the custom ini file ([EtaConfig_14515.ini](#)) from the **File** dropdown.
 - 8 Click **Upgrade**.
EventTracker overwrites [etaconfig.ini](#) file with new settings.
-

Direct Log Archiver / Netflow Receiver

Configuring Direct Log File Archiver

This option helps you archive log files collected from external sources.

To archive log files collected from external sources

- 1 Click the **Admin** dropdown, and then click **Manager**.
- 2 Click the **Direct Log Archiver / NetFlow Receiver** tab.
- 3 Select the **Direct log file archiving from external sources** checkbox, if not selected.
- 4 To purge the log files, enter the number of days in **Purge files after – days** field.
- 5 Select a port from the **Associated virtual collection point** drop-down list.
Assign an exclusive port that is not associated with any collection groups.
- 6 Click **Save**.

For more information, refer

<http://www.prismmicrosys.com/Support/latest%20guides/EventTracker%20v7.0%20Enterprise%20Direct%20Log%20Archiver.pdf>

Vulnerability Scanners

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses. There are a number of types of vulnerability scanners available today, distinguished from one another by a focus on particular targets. While functionality varies between different types of vulnerability scanners, they share a common, core purpose of enumerating the vulnerabilities present in one or more targets. Vulnerability scanners are a core technology component of Vulnerability management.

Source: http://en.wikipedia.org/wiki/Vulnerability_scanner

Qualys Parser

The EventTracker v7.X parser reads the Qualys XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see Table 56), and updates the value of "V" for the managed system.

The root element of a Qualys XML report is named "SCAN". It contains a child element named "IP" for each IP address that was scanned by the vulnerability scanner.

The child objects of "IP" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Qualys XML are:

- 1=Minimal
- 2=Medium
- 3=Serious
- 4=Critical
- 5=Urgent

QUALYS SEVERITY TO EVENTTRACKER WEIGHTAGE MAPPING

Table 53

Qualys Severity	EventTracker Weightage
1 (Minimal)	1 (Low)
2 (Medium)	2 (Medium)
3 (Serious)	3 (High)
4 (Critical)	4 (Serious)
5 (Urgent)	5 (Critical)

Nessus Parser

The EventTracker v7.X reads the Nessus XML (V1 and V2) report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see Table 57), and updates the value of "V" for the managed system.

Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Nessus XML are:

0=Open Port

1=Low

2=Medium

3=High

NESSUS SEVERITY TO EVENTTRACKER WEIGHTAGE MAPPING

Table 54

Nessus Severity	EventTracker Weightage
0 (Open Port)	0 (Undefined)
1 (Low)	1 (Low)
2 (Medium)	3 (High)
3 (High)	5 (Critical)

SAINT Parser

The EventTracker v7.X parser reads the SAINT XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see Table 58), and updates the value of "V" for the managed system.

The root element of a SAINT XML report is named "report". It contains a child element called "details" from which EventTracker extract the vulnerability information. This element contains a child element named "host_info" for each system that was scanned by the vulnerability scanner.

The child objects of "host_info" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the SAINT XML are:

1) **critical** - Critical Problem (Red) – Vulnerabilities which could allow an attacker to gain direct and unassisted read, write, or command execution access, or to create a denial of service.

2) **concern** - Area of Concern (Yellow) – Vulnerabilities which could allow privilege elevation, remote access upon some user action, bypass of security measures, use of the target as an intermediary in an attack, or disclosure of passwords or other information that could be used in an attack, but do not themselves result in direct, unassisted remote access.

3) **potential** - Potential Problem (Brown) – Services or applications which may or may not be vulnerabilities, depending on the version, patch level, or configuration. Further investigation on the part of the administrator may be necessary.

4) **service** - Service (Green) – Any service which is running, regardless of whether or not it is vulnerable.

SAINT SEVERITY TO EVENTTRACKER WEIGHTAGE MAPPING

Table 55

SAINT Severity	EventTracker Weightage
service (Green)	0 (Undefined)
potential (Brown)	1 (Low)
concern (Yellow)	3 (High)
critical (Red)	5 (Critical)

eEye Retina Parser

The EventTracker v7.X parser reads the Retina XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see Table 59), and updates the value of "V" for the managed system.

The root element of a Retina XML report is named "scanJob". It contains a child element called "hosts" from which EventTracker extract the vulnerability information. This element contains a child element named "host" for each system that was scanned by the vulnerability scanner.

The child objects of "host" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Retina XML are:

1) **Information** - A security vulnerability that gives the attacker more information, which then helps him to target his attacks more successfully. These can be directory structures, account names, network addresses, or the internal descriptions and information of other machines.

- 2) **Low** - Low-risk vulnerability usually include vulnerabilities that can be exploited to read files containing public information, or a vulnerability that gives an attacker very minimal access to a remote system.
- 3) **Medium** - Medium Level usually includes vulnerabilities that can be exploited to gain general access to a system. Vulnerabilities that allow attackers to remotely view sensitive files can be categorized here also.
- 4) **High** - Full remote access. A vulnerability that can be exploited to gain total access of a machine remotely falls under this category. These vulnerabilities are extremely severe, and tools to exploit them are usually publicly available.

RETINA SEVERITY TO EVENTTRACKER WEIGHTAGE MAPPING

Table 56

Retina Severity	EventTracker Weightage
Information	0 (Undefined)
Low	1 (Low)
Medium	3 (High)
High	5 (Critical)

Rapid7 NeXpose Parser

The EventTracker v7.X parser reads the Rapid7 NeXpose XML report and extracts vulnerability information from it to adjust the value of "V" for systems managed by EventTracker.

When vulnerability information of a system managed by EventTracker is found in the report, the parser extracts the highest severity value from the vulnerabilities detected on the system, maps it to EventTracker weightage (see Table 60), and updates the value of "V" for the managed system.

The root element of a Rapid7 NeXpose XML report is named "SCAN". It contains a child element named "IP" for each IP address that was scanned by the vulnerability scanner.

The child objects of "IP" element contain OS and vulnerability information. Each vulnerability detected on target has severity value associated with it. The possible severity values defined in the Rapid7 NeXpose XML are:

- 1=Minimal
- 2=Medium
- 3=Serious
- 4=Critical
- 5=Urgent

RAPID7 NEXPOSE SEVERITY TO EVENTTRACKER WEIGHTAGE
MAPPING

Table 57

Rapid7 NeXpose Severity	EventTracker Weightage
1 (Minimal)	1 (Low)
2 (Medium)	2 (Medium)
3 (Serious)	3 (High)
4 (Critical)	4 (Serious)
5 (Urgent)	5 (Critical)

Enabling NetFlow Receiver

This option enables you to enable netflow receiver and read netflow logs.

To enable NetFlow receiver

- 1 Click the **Admin** dropdown, and then click **Manager**.
- 2 Click the **Direct Log Archiver/Netflow Receiver** tab.
- 3 Check the **Enable netflow receiver** option.
EventTracker enables the **Netflow data storage folder** field.
- 4 Type the path of the folder or click the **Browse** button to select the folder.
By default, netflow receiver receives netflow logs through 9991, 9992, and 9993 ports.

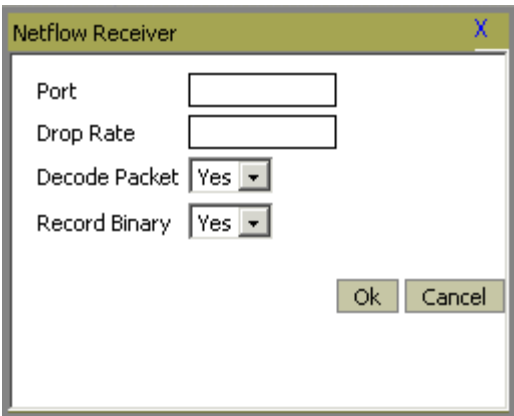
Adding Netflow Receiver Port

This option helps to add netflow receiver port.

To add Netflow Receiver port

- 1 Click **Add**.
EventTracker displays the **NetFlow Receiver** pop-up window.

Figure 183
NetFlow Receiver



The image shows a 'NetFlow Receiver' dialog box with a title bar containing a close button (X). The dialog contains four input fields: 'Port' and 'Drop Rate' are text boxes; 'Decode Packet' and 'Record Binary' are dropdown menus, both currently set to 'Yes'. At the bottom right, there are 'Ok' and 'Cancel' buttons.

Table 58

Field	Description
Port	Type the netflow receiver port number.
Drop Rate	Drop Rate configures a sampling rate. This is a 'REG_MULTI_SZ' key with an integer value per port. The meaning of the value is that one packet in 'Drop Rate' packets will be discarded. Hence 'Drop Rate' of 2 would cause every other packet to be discarded. In this version sampling is deterministic (not probabilistic). In the absence of this registry entry, the default will be taken to be 0.
Decode Packet	Instruct the service how to record the sampled data. The key 'DecodePacket' is also of type 'REG_MULTI_SZ' and is a list of Boolean values ('true'/'false') that indicate whether the packets received on the corresponding port should be decoded and written to the 'netflowcollectorXXXX.txt' file.
Record Binary	Instruct the service how to record the sampled data. Setting these values to 'true' will cause the received packets to be written to files simply as binary data. Only one of 'Decode Packet' or 'Record Binary' may be both true for any particular port. If both are set to 'true' the Port will act as if 'Decode Packet' was set to true and 'Record Binary' was set to false. In the absence of these registry values the default will be to assume the 'Decode Packet' value is true and the 'Record Binary' value is false.

- 2 Select/enter appropriately in the relevant fields, and then click **OK**.
- 3 Click **Save**.

Agent Settings

Configure Agent File Transfer Settings

This option enables you to configure agent file transfer settings.

To configure agent file transfer settings

- 1 In the **Manager Configuration** page, click the **Agent Settings** tab.
- 2 Select the **Allow direct agent file transfers** checkbox, if not selected.
Associated virtual collection point is the port that you have configured for Direct Log Archiver.
By default, EventTracker stores the files transferred by the agents in the ...\\Program Files\\Prism Microsystems\\EventTracker\\DLA folder.
- 3 In the **Data Store Folder** field, type the path for new folder if you wish to change the file transfer location.

(OR)

Click the **Browse** button to navigate and select a folder.

- 4 Click **Save**.
-

Configuring Config Assessment Settings

- 1 In the **Manager Configuration** page, click the **Agent Settings** tab.
 - 2 Select the **Encrypt Data Transfer** checkbox, if not selected.
By default, EventTracker stores the SCAP files in the [...\Program Files\Prism Microsystems\EventTracker\SCAP\](#) folder.
 - 3 In the **Data Store Folder** field, type the path for new folder if you wish to change the file transfer location.
(OR)
Click the **Browse** button to navigate and select a folder.
 - 4 Click **Save**.
-

Configuring E-mail Settings

This option will help you to configure email settings. These are mandatory configuration settings to "Deliver report via E-mail" or "Notify report generation via E-mail" upon generation of scheduled reports. Additionally, to "Send via E-mail" the published reports.

- 1 In the **Manager Configuration** page, click the **E-Mail configuration** tab.

Table 59

Field	Description
SMTP Server	Type the name or IP address of your enterprise mail server.
Port	Type a valid SMTP server port number.
From E-mail id	Type a valid sender e-mail address.
To E-mail id	Type a valid recipient e-mail address.
Email attachment maximum size	Type the maximum size of attachment file in terms of MB. The default size will be 5 MB.
Enable authentication	Provides an access control mechanism. It can be used to allow legitimate users to relay mail while denying relay service to unauthorized users, such as spammers. Select this checkbox and type valid administrator user name and password.
Test E-mail	Click to check whether you have provided valid data.

Field	Description
	EventTracker displays the confirmation message box. Click OK to continue. EventTracker displays "success" message if the configuration is correct and "failed" message if the configuration is not correct.

- 2 Provide the details in required fields, and then click the **Save** button.

Manage Email Accounts

All the Email Ids configured in alerts, reports, and flex reports can be managed from this Email search utility. The Email Ids can be replaced with a new Email Id or removed if it is no more in use or invalid address.

- 1 In the **Manager Configuration** page, click the **E-Mail configuration** tab.
- 2 Fill the required information to configure the SMTP server for sending email, and then click the **Save** button.
- 3 Click the **Manage email** hyperlink.

EventTracker displays **Email search utility** window.

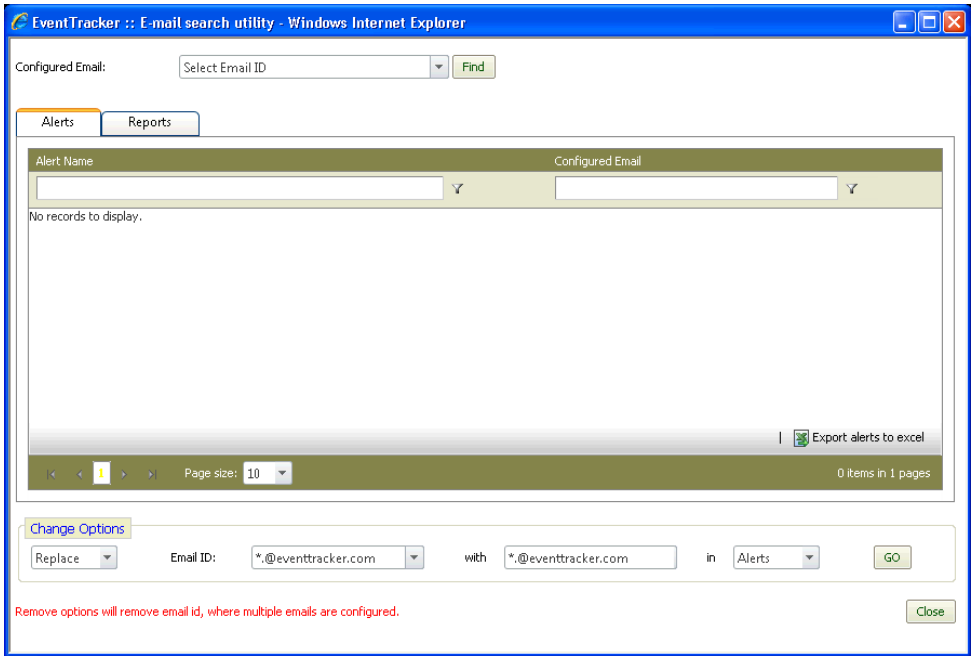


Table 60

Field	Description
Configured Email	The list of all configured email Ids.
Alerts	The list of alerts configured with the selected email Id.
Reports	The list of reports configured with the selected email Id.

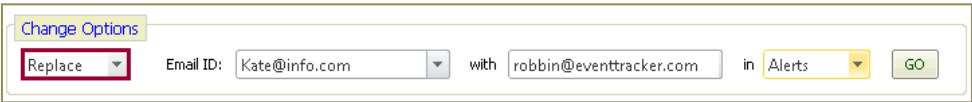
Field	Description
Export alerts to excel / Export reports to excel	Click to export the alerts or reports along with the configured email Id.
Change Option	Remove or replace the configured email Id.

- 4 From **Configured Email** dropdown, select the required email Id, and then click the **Find** button.

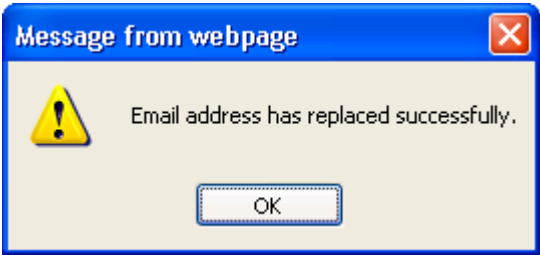
The alert(s) and report(s) configured with the email Id will be displayed under **Alerts** and **Reports** tab, respectively.

To Replace the Email Id

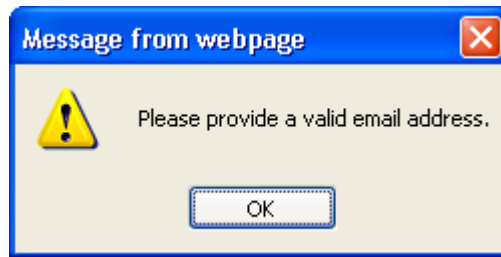
- 1 Click the **Manage email** hyperlink.
EventTracker displays 'E-mail search utility' window.
- 2 In the **Change Options** pane, select **Replace** from the dropdown, if not selected.
- 3 From the **Email ID** dropdown, select the Email Id to be replaced.
- 4 In **With** field, type the Email Id to be replaced.
- 5 In the 'in' field select where the Email Id is to be replaced. The options are in **Alerts** or in **Reports**.



- 6 Click the **Go** button.
EventTracker displays confirmation message box.
- 7 Click the **OK** button.
EventTracker displays success message box.



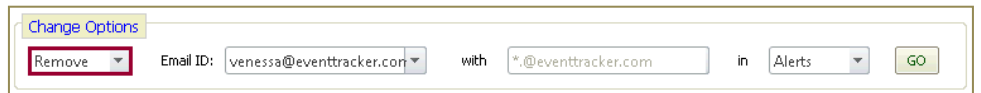
If you have provided any special character or wrong Email Id then EventTracker will display the error message.



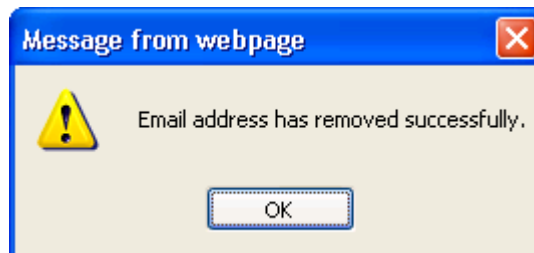
- 8 Click the **OK** button in the success message box.
- 9 To verify the replacement, click the **Configured Email** dropdown, select the replaced Email address, and then click the **Find** button.
EventTracker will display the alerts or reports configured with the selected Email Id.

To Remove the Email Id

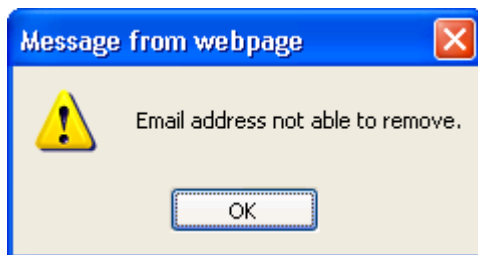
- 1 Click the **Manage email** hyperlink.
EventTracker displays 'E-mail search utility' window.
- 2 In the **Change Options** pane, select **Remove** from the dropdown.
- 3 From the **Email ID** dropdown, select the Email Id to be removed.
- 4 In the 'in' field select where the Email Id is to be removed. The options are in **Alerts** or in **Reports**.



- 5 Click the **Go** button.
EventTracker displays confirmation message box.
- 6 Click the **OK** button.
EventTracker displays success message box.



If only one report or alert is configured with the selected Email address then EventTracker will not allow to remove the Email address.



- 7 Click the **OK** button in the success message box.
-

Configuring StatusTracker Settings

- 1 Click the **Admin** dropdown, and then click **Manager**.
 - 2 Click the **StatusTracker** tab.
 - 3 In **Purge frequency for StatusTracker** field, enter the number of days.
The StatusTracker polling summary data will be purged after the specified number of day(s).
 - 4 Check the **Synchronize discovery with EventTracker** option.
Select this option if you wish to populate the groups along with their respective systems when "Auto discover" is carried out in System Manager.
 - 5 Enter the string name in **Community string for SNMP devices** field to configure the community string for SNMP devices.
-

Chapter 10

Configuring Alerts and Alert Notifications

In this chapter, you will learn how to:

- [Add Custom Alerts](#)
- [Add pre-defined Categories as Alerts](#)
- [Manage Categories](#)
- [Modify Alert Details](#)
- [Delete Alerts](#)
- [Configure Alert Actions – Manager Side](#)
- [Execute Remedial Action at EventTracker Manager System](#)
- [Execute Remedial Action at EventTracker Windows Agent System](#)

Alerts

EventTracker generates an alert when a critical event occurs, such as security breaches, performance problems, etc. Configure an unlimited number of rule-based alerts with customizable event criteria including support for event-fired automatic (custom) actions for any defined event.

- Out of the Box alerts for the most common predefined alert condition
 - Ability to create your own alert conditions
 - Reliable framework for alerts
 - Ability to minimize false positive
 - Firing automatic actions as a receipt of event can increase system's availability
-

Risk Metrics

EventTracker 'Risk Metrics' considers three factors to calculate Risk (R). This calculation will be performed just before an alert is raised. Alert notification is sent only when the risk is greater than or equal to the threshold.

T	Threat level (how severe the Alert is) assigned while creating Alerts
A	Asset value of the system (how important or critical the computer is) set through the System Manager
V	Vulnerability (how vulnerable the computer is) automatically updated using third party vulnerability assessment reports.

Example #1:

Day 1
System Type: Server
Threat level: Medium
Asset value: Medium
Vulnerability: High

Alert notification is sent since it is found to be highly vulnerable by running the vulnerability scanner.

Example #2:

Day 2
System Type: Server
Threat level: Medium
Asset value: Medium
Vulnerability: Low (system is hardened by applying hotfixes, patches, & service packs)

Alert notification is not sent since it is found to be not vulnerable by running the vulnerability scanner.

To know more, click the following links

Qualys Parser

Nessus Parser

SAINT Parser

eEye Retina Parser

Add Custom Alerts

This option enables you to configure alert, add events to alert, and configure alert actions.

To add custom alerts

- 1 Click **Admin** dropdown, and then click **Alerts**.

EventTracker displays **Alert Management** page.

Figure 184
Alert Management

Alert Management

Search:

Go

Page Size: 25

1 2 3 4 5 6 7 8 9 10 ... >>

<input type="checkbox"/>	Alert Name ▲	Threat level	Active	Beeper	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
<input checked="" type="checkbox"/>	Active Directory: Group policy changed	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Admin Interactive/Remote Interactive login failure	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Admin Interactive/Remote Interactive login success	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Administrative logon failure	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Administrative logon success	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Altiris	Undefined	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ArubaOS: Accounting error	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ArubaOS: Anomaly detection	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ArubaOS: AP Flood attack	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ArubaOS: Authentication failed	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	ArubaOS: Certificate authentication error	Undefined	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	ArubaOS: Certificate conversion error	Undefined	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	ArubaOS: Certificate downloading failed	Undefined	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

***Click 'Activate Now' after making all changes

Activate Now

Add alert

Delete

Table 61

Field	Description
Search	Type the search string and then click GO . This helps to easily locate the alert you are looking for.
Page Size	Select an option from this drop-down list to display the maximum number of alerts in a page.
Alert Name	Name of the alert. Click the hyperlink to modify alert details.
Threat level	Severity of the alert.

Field	Description
Active	Select or clear the checkbox to activate or deactivate the alert.
Beep	Select this checkbox to configure audible alert notification.
E-mail	Select this checkbox to configure e-mail alert notification. The SMTP server should be configured to send Email.
Message	Select this checkbox to configure console message alert notification.
RSS	Select this checkbox to configure notification through RSS Feeds.
Forward as SNMP	Select this checkbox to forward alert notification as an SNMP trap.
Forward as SYSLOG	Select this checkbox to forward alert notification as a SYSLOG message.
Remedial Action at Console	Select this checkbox to configure custom action to be executed on receipt of an event at the manager side.
Remedial Action at Agent	Select this checkbox to configure custom action to be executed on receipt of an event at the agent side. You execute these actions only on Windows systems where agents are deployed. You cannot execute these actions on NIX systems where agent less monitoring is deployed.
Activate Now	Click to activate the selected alert.
Add alert	Click to add custom alert.
Delete	Select the checkbox against the alert that you want to delete, and then click Delete . Select the checkbox adjacent to the 'Alert Name" column to select all Alerts.

- On the **Alert Management** page, click the **Add alert** button to add new alert. EventTracker displays the **Alert configuration** page.

Alert configuration

Alert Name:

Threat level:

Undefined

Threshold level:

Medium

Show in:

none

Previous

Event Details --> Event Filter --> Custom --> Systems --> Actions

Next

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
0	0						

Add

Edit

Delete

Finish

Cancel

OR

Click the name of the alert that you wish to modify.
EventTracker displays the **Alert configuration** page.

Figure 185
Alert Configuration

Alert configuration

Alert Name:

Administrative logon failure

Threat level:

High

Threshold level:

Medium

Show in:

none

Previous

Event Details --> Event Filter --> Custom --> Systems --> Actions

Next

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
Security	Audit Failure	0	675	Security	Administrator		
Security	Audit Failure	0	529	Security	Administrator		
Security	Audit Failure	0	676	Security	Administrator		
Security	Audit Failure	0	672	Security	Administrator		
Security	Audit Failure	0	4771	Microsoft-Windows-Security-Auditing	(Account Name:\t\Administrator)		
Security	Audit	0	4625	Microsoft-Windows-Security-	Account For Which Logon Failed:(\x0-\xFF)\0,\XAccount		

Add

Edit

Delete

Finish

Cancel

Table 62

Fields	Description
Threat level	Select severity of the alert.
Threshold level	Alert notification is sent when the risk is greater or equal to the threshold.
Show in	Select 'Compliance Dashboard' from dropdown to view the selected alert details in the compliance dashboard.

- 3
- Type the new alert name in the **Alert Name** field. Example: My Alert
- 4
- Select the severity of threat from the **Threat level** drop-down list.

- 5 Select the threshold from the **Threshold level** drop-down list.
- 6 If you wish to see the alert in compliance dashboard then select 'Compliance Dashboard' in **Show in** dropdown.
- 7 Click the **Add button** to add event details.

EventTracker displays the **Add Event** dialog box.

Figure 186
Add Alert Event

Add Event

Log Type :

Event Type :

Category :

User :

Event Id :

Source :

Match in Description :

Description exception :

To provide special characters like """, """, """, """, etc. prefix the char with a backslash. Example: ""\" for ""\" and ""\" for ""\".

Add

Cancel

Table 63

Field	Description
Log Type	It describes the type of log to be monitored.
Event Type	Classification of event severity: Error, Information, Warning in the System and Application logs; Audit Success or Audit Failure in the Security log. Select an event type from the drop-down list.
Category	Classification of the event by the event source. This information is primarily used in the security log. For example, for security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in Group Policy. Type the category number in this field. This field supports numeric data type only.
User	Type the name of the user.
Event Id	A number identifying a particular event. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems. Type the event ID number in this field. This field supports numeric data type only.

Field	Description
Source	The software that logged the event, which can be either a program name such as "SQL Server," or a component of the system or of a large program such as a driver name. For example, "Elnkii" indicates an EtherLink II driver. Type the source in this field.
Match in Description	Type a sub-string of the description that needs to be matched. EventTracker supports multiple strings separated by the following operands. && stands for AND condition. stands for OR condition. If you type Successful Logon && New Trusted Domain Removing Trusted Domain, EventTracker will filter out the events that are matching Successful Logon, (AND) New Trusted Domain (OR) Removing Trusted Domain.
Description exception	Type a sub-string of the description that needs to be exempted.

Table 64

Event Type	Description
Error	A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error will be logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning will be logged.
Information	In event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
Audit Success	An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.
Audit Failure	An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
Verbose	A Verbose event is a debugging trace. (Applies only to Vista)
Critical	A critical event is a fatal error or application crash. (Applies only to Vista)

Table 65

Event log type	Log file	Function	Availability
Application log	AppEvent.evt	Records events as determined by each software vendor	All Windows systems

Event log type	Log file	Function	Availability
Security log	SecEvent.evt	Records events based on how audit policy is configured	All Windows systems
System log	SysEvent.evt	Records events for Windows operating system components	All Windows systems
Directory Service log	NTDS.evt	Records events for Active Directory	Domain controllers only
DNS Server log	DnsEvent.evt	Records events for DNS servers and name resolution	DNS servers only
File Replication Service log	NtFrs.evt	Records events for domain controller replication	Domain controllers only

- 8 Type appropriately in the relevant fields, and then click **Add**.
- 9 Click **Event Filter** hyperlink (OR) click **Next ➡**.
EventTracker displays the **Event Filter** page.
- 10 Click **Add** to add event details for the event filter.
- 11 Type appropriately in the relevant fields, and then click **Add**.
- 12 Click **Custom** hyperlink (OR) click **Next ➡**.
EventTracker displays the **Custom** page.

Figure 187
Custom

Alert configuration

Alert Name:

Threat level: Threshold level: Show in:

Time Interval

Alerts are valid only during this Time interval

☒ Apply All Time

☐ Apply between these time

from:

to:

Alert based on count

Raise the alert only if the same Event occurs for the specified count within specified duration

☐ Enable

Raise alert for event count: Duration: in seconds

Archive Alert

☒ Store this alert in Alert Archives

Finish

Cancel

Table 66

Field	Description
-------	-------------

The default value for **Raise alert for event count** is 2 and **Duration** is 3600 in seconds.

Field	Description
Apply All Time	If selected, alerts actions are executed for events occurred all through the day (24 hours).
Apply between these time	If selected, alerts actions are executed for events occurred during the specified time frame.
Alert based on Count	This option lets you to receive alert notification only when the same event occurs for the specified number of times within the specified duration. Check the Enable option, to provide the event count and duration.
Archive Alert	Select the Store this alert in Alert Archives option to store the alert in the 'Alerts Archives'. Archived alerts will be used for the alert analysis.

13 Select **Apply All Time** option.

(OR)

Select the **Apply between this time** option, and then select **From** and **To** time from the calendar control.

14 In **Alert based on count** pane, check the **Enable** option, provide the number of event count in the **Raise alert for event count** field, and then provide the time in seconds in the **Duration** field.

15 Click **Systems** (OR) click **Next** ➡.

EventTracker displays the **Systems** page.

By default, EventTracker selects the All Systems checkbox to apply the Alert to all monitored groups/systems. Clear this checkbox to select groups/systems.

16 Select the Groups / Systems / All Systems for which the alert is to be monitored.

Figure 188
Select
system(s)/groups

The screenshot shows the 'Alert configuration' dialog box with the 'Systems' tab selected. At the top, there are fields for 'Alert Name' (My Alert), 'Threat level' (Undefined), 'Threshold level' (Medium), and 'Show in' (none). A breadcrumb trail at the top right reads: 'Previous Event Details --> Event Filter --> Custom --> Systems --> Actions Next'. Below the tabs, there are three radio buttons: 'Groups', 'Systems', and 'All Systems' (which is checked). A search bar labeled 'Search System(s):' is present, followed by a list of systems: 'Default' and 'TOONS'. At the bottom right, there are 'Finish' and 'Cancel' buttons.

17 Click **Actions** hyperlink (OR) click **Next** ➡.

Figure 189
Action

To configure an alert, action is not mandatory. **Alert actions** can be configured at any point of time.

EventTracker displays the **Actions** page.

Alert configuration

Alert Name:

Threat level: Threshold level: Show in:

[Previous Event Details](#) --> [Event Filter](#) --> [Custom](#) --> [Systems](#) --> [Actions](#) **Next**

E - mail | Rss | Beep | Net message | SNMP | syslog | Agent Remedial Action | Console Remedial Action

Email Configuration

An e-mail message will be sent (comma separation for multiple addresses).

To:

Subject:

- 18 Select the type of action from the respective tabs.
- 19 Configure the selected action appropriately.
- 20 Click **Finish**.

EventTracker adds the newly created alert and displays it on the **Alert Management** page.

Figure 190
Alert Management

Alert Management

Search:

Page Size:

Alert Name▲▲	Threat level	Active	Beep	E-mail	Message	Rss	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
<input type="checkbox"/> MExchange: Exchange Server database disk full	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Exchange Server database error	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Exchange server database missing or corrupt	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Exchange services not running	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Information Store service problem	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: IS service cannot be started	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: IsAlive check failed for clustered resource	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Log disk is full	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Logon failure on mailbox database	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Public Folder storage limit exceeded	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Server cannot handle influx of mail	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Unable to start exchange server	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> My Alert	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Newly added alert

***Click 'Activate Now' after making all changes

- 21 To activate the newly added alert, select the checkbox under **Active** column.
- EventTracker displays the success message pop-up window.

Figure 191
Alert Configuration

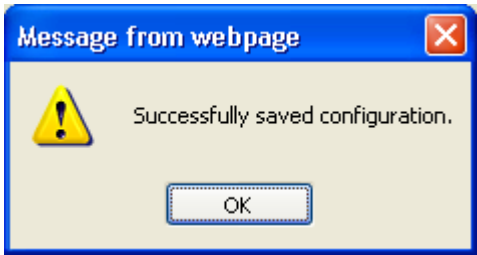


Figure 192
Alert Configuration

- 22 Click **OK**.
EventTracker saves the alert configuration.

 **NOTE**

The configured alert details can be modified/edited at any point of time. On the **Alert Management** page, click the alert name to be modified/edited. Make the necessary changes in **Alert Configuration** page, and then click the **Finish** button to save the changes.

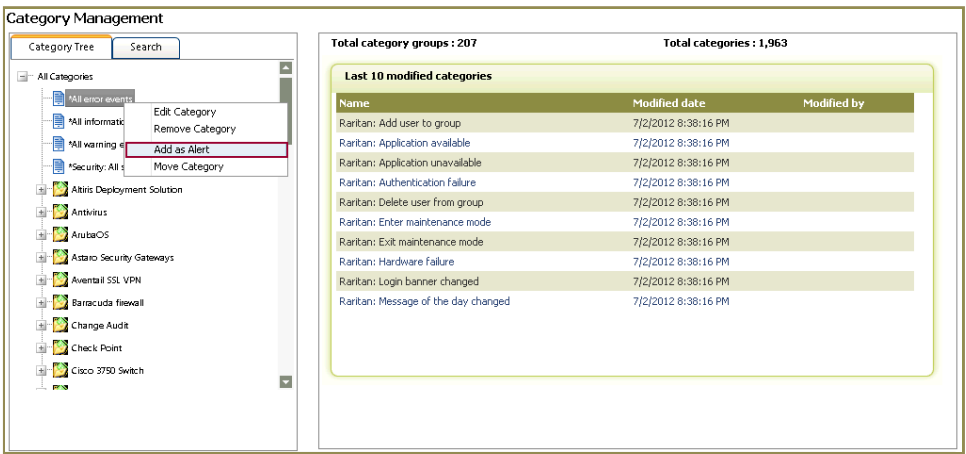
Add Pre-defined Categories as Alerts

This option helps to add pre-defined categories as alerts.

To add pre-defined Categories as alerts

- 1 Click the **Admin** dropdown, and then click **Category**.
EventTracker displays the **Category Management** page.

Figure 193



- 2 Right-click the category that you wish to add as an alert.

- 3 From the shortcut menu, select **Add as Alert**.
 - 4 EventTracker displays the **Alert Management -> Event Details** page.
Complete the alert configuration process as described in [Add Custom Alerts](#) section.
-

Deleting Alerts

This option enables you to delete Alerts.

To delete Alerts

- 1 On the **Alert Management** page, select the alert to be deleted.
 - 2 Click the **Delete** button.
-

Configuring Alert Actions – Manager Side

You can associate an alert action with pre-defined alerts by selecting appropriate checkboxes on the **Alert Management** page.

This option enables you to configure alert actions that are to be executed at the EventTracker manager system.

To configure alert actions

- 1 Configure an alert as explained in the [Add Custom Alerts](#).
- 2 Click an appropriate tab to configure alert actions.

NOTE

You have the liberty to set more than one alert action.

Configure E-mail Alert Action

This option enables you to configure an E-mail(s) to send as an alert action.

To configure E-mail alert action

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **E – mail** tab.
OR
On the **Alert Management** page, click the checkbox under **E-mail** column.
EventTracker displays the Email dialog box.

Figure 194
Email

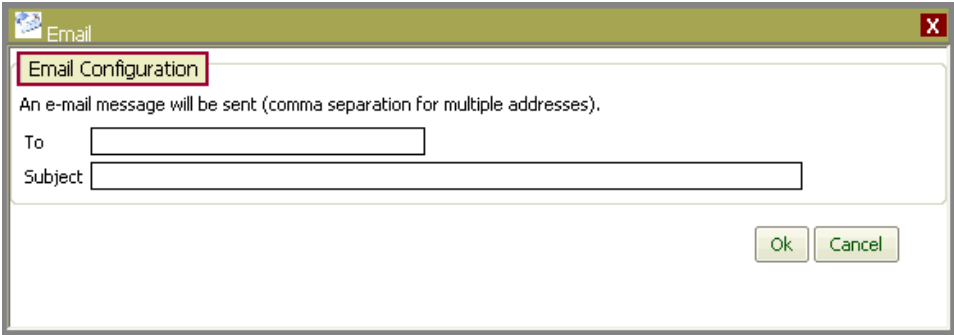


Table 67

Field	Description
From	Type a valid sender e-mail address. Use comma as a separator to provide multiple addresses.
Subject	Provide a subject line for the Email.

- 2 Enter required details.
- 3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.
OR
In the **Email** dialog box, click **OK**.
- 4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.

FAQ: I SETUP AN EMAIL ALERT AND IT IS NOT WORKING. WHAT SHOULD I DO?

Please crosscheck the following.

- The SMTP server mentioned must be accessible from the Console system. That is either the system must be able to access Internet or the SMTP server must be reachable over the LAN.
- Ensure valid email addresses are provided in both "To Address" and "From Address".

Configure Audible Alert Action

This option enables you to configure audible alert action.

To configure audible alert action

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **Beep** tab.
OR
On the **Alert Management** page, click the checkbox under **Beep** column.

Figure 195
Beep

EventTracker displays the **Beep** dialog box.

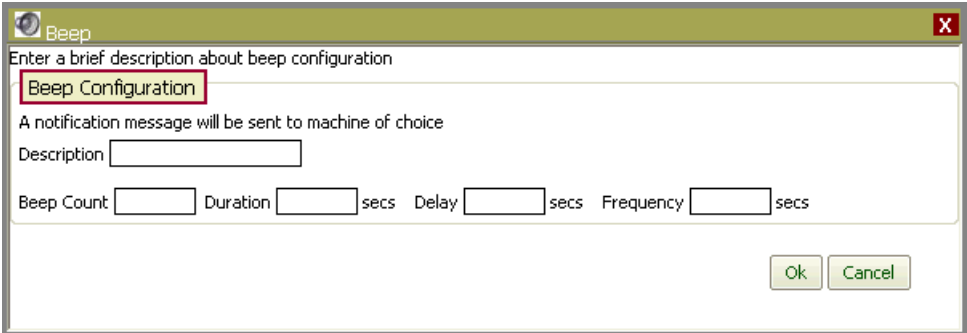


Table 68

Field	Description	
Description	Type a brief description about the beep action.	
Beep Count	Type the number of beeps that should be generated at the PC speaker.	These fields support numeric data type only.
Duration	Type how long should the beep be sustained.	
Delay	Type the time interval to pause between consecutive beeps.	
Frequency	Type the frequency (Hertz) of the beep sound.	

- 2 Enter appropriate values in the relevant fields.
- 3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.
OR
In the **Beep** dialog box, click **OK**.
- 4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.

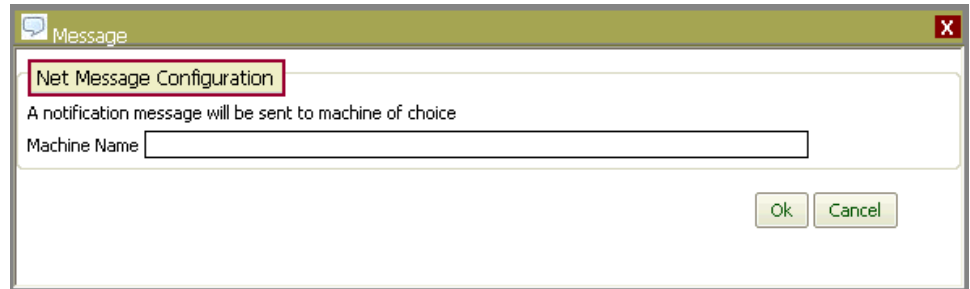
Configure Console Message Alert Action

This option enables you to configure a console message alert. A notification message will be sent to the selected machine.

To configure console message alert action

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **Net message** tab.
OR
On the **Alert Management** page, click the checkbox under **Message** column.
EventTracker displays the **Message** dialog box.

Figure 196
Message



- 2 Type the name of system in **Machine Name** field.
- 3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.
OR
In the **Message** dialog box, click **OK**.
- 4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.

Configure RSS Alert Notification

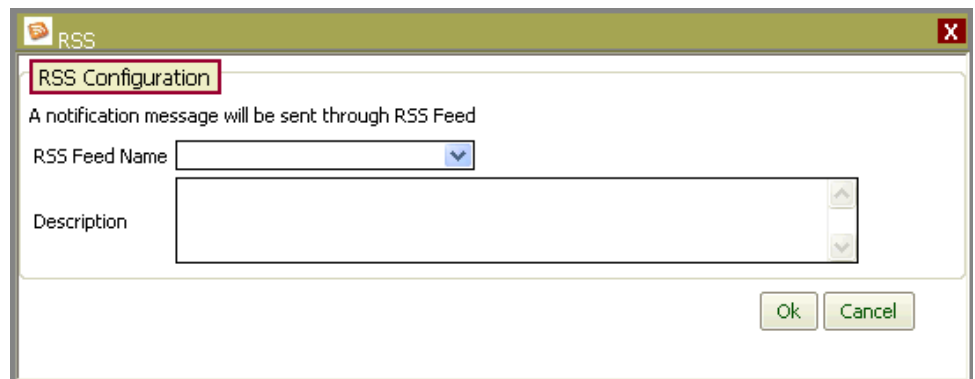
This option helps you to get notified via RSS, alerts raised by EventTracker for configured events.

To configure RSS Alert notification

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **RSS** tab.
OR
On the **Alert Management** page, click the checkbox under **RSS** column.
EventTracker displays the RSS dialog box.


Figure 197
RSS

To configure
RSS Feeds, go
to **Admin**
dropdown >>
Click **RSS**.



- 2 Select RSS Feed from the **RSS Feed Name** drop-down list.

- 3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.
OR
In the **RSS** dialog box, click **OK**.
- 4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.

 **NOTE**

You must create RSS Feeds prior to using this feature.

Forward Events as SNMP Traps

All incoming events are compared with the configured alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as an SNMP trap to the specified destination.

To forward events as SNMP traps

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **SNMP** tab.
OR
On the **Alert Management** page, click the checkbox under **Forward as SNMP** column.
EventTracker displays the **SNMP** dialog box.

Figure 198
SNMP

SNMP

Forward Events as SNMP traps

Select destination and Port No to which Event will be sent as SNMP trap

Trap Destination

Port No

Ok Cancel

Table 69

Field	Description
-------	-------------

Field	Description
Trap Destination	Type the IP address or host name.
Port No	Type the UDP port number in this field. This field supports numeric data type only.

- 2 Type appropriately in the relevant fields.
 - 3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.
OR
In the **SNMP** dialog box, click **OK**.
 - 4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.
-

Forward events as syslog messages

All incoming events are compared with the configured alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as a syslog message to the specified destination.

To forward events as Syslog messages

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **syslog** tab.
OR
On the **Alert Management** page, select the checkbox under **Forward as syslog**.
EventTracker displays the **syslog** dialog box.

Figure 199
syslog

Table 70

Field	Description
Mode	Select either TCP or UDP as the transport protocol mode.
Load last selection	Click to load the last saved configuration of a syslog message.
Destination	
syslog Destination	Type the IP address or host name.
Port No	Type the port number corresponding to the transport mode selected.
syslog Details	
RFC 3164 syslog facility type	Return facility value from a received and processed syslog message. This is the text representation of the facility.
RFC 3164 syslog severity type	Return severity value from a received and processed syslog message. This is the text representation of the severity.
Event Properties	Select the event properties to be included in the description of the syslog message. EventTracker by default selects Event ID, Source, and Description options. You can select properties as per your choice.
syslog Format	

Field	Description
Replace new lines (CRLF) with	Replaces the newline characters in the syslog message with tab or space.
Insert prefix	Check Insert Prefix option and then provide the prefix. The system messages sent to the syslog device inserts this prefix to all the messages it intercepts on their way to the message file.
Include priority code	Each syslog message is one line. A message can contain a priority code, marked by a digit enclosed in < > (angle braces) at the beginning of the line. The priority code represents both the Facility and Severity of the message.

- 2 Select/enter appropriately in the relevant fields.
- 3 Click **OK**.

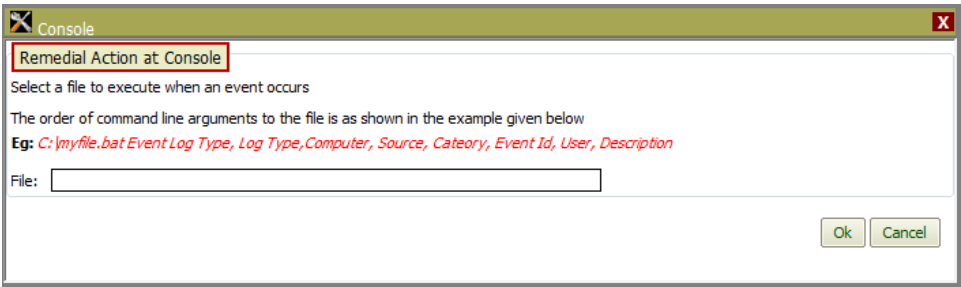
Executing Remedial Action at EventTracker Manager Console System

This option enables you to configure custom action to be executed on receipt of an event at the manager system.

To configure remedial action at the manager console

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **Console Remedial Action** tab.
OR
On the **Alert Management** page, click the checkbox under **Remedial Action at Console** column.
EventTracker displays the **Console** dialog box.

Figure 200
Console



- 2 Type the path of the custom action file in the **File** field.
- 3 Click **OK**.

Agent side remedial action helps to perform remedial actions at the system where EventTracker agent is installed.

Executing Remedial Action at EventTracker Windows Agent System

Though EventTracker is shipped with predefined alerts that are applicable to all monitored systems irrespective of O/S and mode of monitoring (Agent based or Agent less), to get alert notification messages you need to explicitly configure alert actions. While configuring alert actions it is left to your discretion to include and exclude systems. Same rule holds good for user-defined alerts. Note that remedial actions can be executed only on systems where EventTracker agent has been deployed.

Excluding systems for alert actions doesn't mean that you are excluding them from monitoring. EventTracker logs all events that occur in monitored systems into the database, you can plow through the data by performing Log Search.

So, utilize this feature judiciously to draw maximum benefits.

To configure remedial action at the agent system

- 1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **Agent Remedial Action** tab.

OR

On the **Alert Management** page, click the checkbox under **Remedial Action at Agent** column.

EventTracker displays the **Agent** dialog box.

Figure 201
Agent

Table 71

Field	Description
Custom Script	Type the name of the script in Script Name field. Script files are stored in the default EventTracker Agent installation path typically ...\\Program Files\\Prism Microsystems\\EventTracker\\Agent
Restart	Type the name of the service that you want to restart in Service

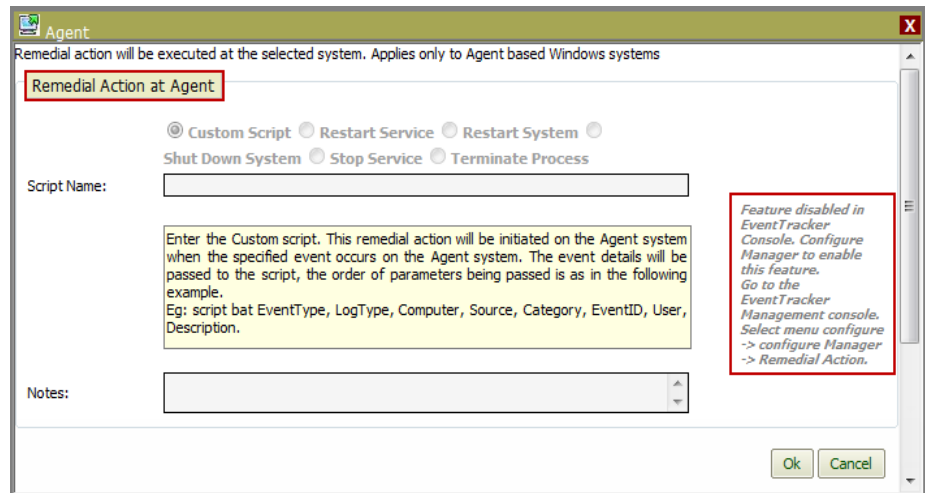
Field	Description
Service	Name field.
Restart System	This option will restart the agent system on the occurrence of the configured event ID.
Shut Down System	This option will shut down the agent system on the occurrence of configured event ID.
Stop Service	Type the name of the service that you want to stop in Service Name field.
Terminate Process	You can configure this action only for events 3217, 3218, 3221, 3223, and 3226.

To enable remedial action at manger console, click Admin dropdown >> Select **Manager** >> Check **Enable Remedial Action** option >> Click **Save** button.

- 2 Select an appropriate remedial action option.
- 3 Type appropriate description in the **Notes** field for future reference.
- 4 Click **Ok**.

If the **Enable remedial action** option is not selected in the 'Manager Configuration' page, EventTracker will display actions window with appropriate message to enable remedial action.

Figure 202
Agent



Edit Alert Actions

This option enables you to edit the alert actions.

To edit alert actions

- 1 On the **Alert Management** page, click the alert name for which you wish to edit the alert actions.
- 2 On the **Alert configuration** page, click **Actions** hyperlink.
- 3 Click appropriate tab(s) to edit the alert action(s).

- 4 Click the **Finish** button to save the changes.
 - 5 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.
-

Fault Monitoring/Alerting/Acting

Alerting is a reactive mechanism against critical events collected in EventTracker. The responsibility lies squarely with the user to configure required notifications like e-mail, beep, messages, or custom actions.

If configured properly, notification mechanism spontaneously notifies the users about the events occurred in all monitored systems that include Windows, non-Windows, Agent based and Agentless systems.

Notifications contain summary of the incident that helps users to investigate the root cause and explore efficient ways to take preventive and remedial measures.

Upon receiving a notification, the security personnel should act promptly to avert any disastrous consequences. What happens if the security person is not aware of the notification?

Is it not good to guard against mishaps than to suffer unnecessarily? Yes, it is always wise to be so. EventTracker provides the necessary facilities to automate remedial actions at the manager Console and remote systems as well, where agents are deployed.

Remedial Actions

Remedial Actions are automated corrective actions taken to mitigate issues that occur at the **Manager** and **Agent** systems.

Remedial actions enable you to:

- Block unauthorized use of PC device access
 - Protect enterprise network against threats posed by portable storage media
 - Enumerate and kill processes that cause havoc
 - Minimize maintenance effort
 - Maximize uptime
-

How it works

Upon receiving Events that requires user's attention, EventTracker can be configured to

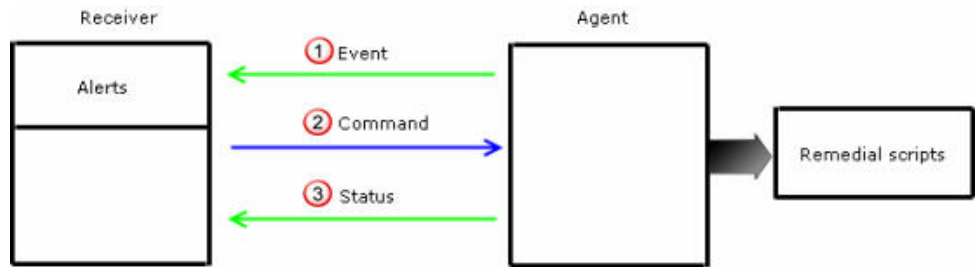
- Raise a beep sound from the PC speaker
- Send e-mail to one or more recipients

- Send network message to specific devices connected to the network
- Forward events as Traps to specific devices

These traditional notifications are good enough to analyze the impact and severity of events. However, what is required is action.

- Execute remedial actions at Manager Console (Custom action in earlier versions) option helps to automate remedial action at the Manager Console.

Figure 203
Remedial Action



Now you may question

- Is it possible to remedy the incidents that occur at remote Agent systems where real action is required?
- Could I execute actions on both Agent based and Agent-less systems?
- Could I execute actions on non-Windows systems?
- Could I execute scripts on remote systems? If so, should those scripts be present locally in all those systems?
- What are the custom actions could I perform on remote systems?
- Do I need any special privileges to perform actions on remote machines?

The answer is straight and simple. Through 'Agent side remedial action" feature, custom action such as blocking USB ports or running scripts is possible, provided

- Remote system should be running Windows O/S (presently non-Windows O/S are not supported).
- You cannot execute custom actions on Agent less systems.
- If you execute scripts on multiple systems, the scripts should be present locally in each system in the EventTracker install directory, typically (... \Program Files \Prism Microsystems \EventTracker \Agent \Script).
- Following are the custom actions you could perform on remote systems
 - Run custom script
 - Restart Service
 - Restart System
 - Shutdown system
 - Stop Service

- Not really needed at this point, as you have already deployed the agent with adequate privileges.

Table 72

Remedial Actions Events & Traps

Remedial Action Events and Traps Field
Manager Side: This event is generated and logged at the Manager side
Event ID = 2035 Event Type = Information Desc = Matched Remedial action request. Initiating Remedial Action Type: <n> on system <system>
Agent side: The Agent forwards these traps to the Manager as acknowledgement.
Event ID = 3234 Usage = Remedial Events Event Type = Information Desc = Received Remedial action request for <Action Type> action.
Event ID = 3235 Usage = Remedial Events Event Type = Information Desc = Successfully initiated <Action Type> action.
Event ID = 3236 Usage = Remedial Events Event Type = Error Desc = Failed to initiate <Action Type> Remedial action.

How Remedial Actions Help

Easily configure group-based protection.

You can organize computers into different groups and specify different rule sets to allow or disallow access to PC devices.

Enable Remedial Action

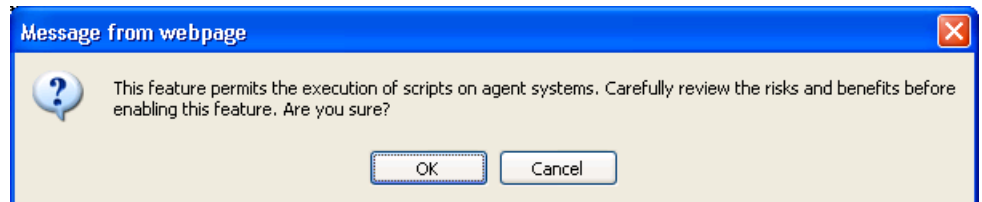
It is mandatory to enable remedial action at Manager Console. Otherwise, you cannot execute remedial action at the Agent systems.

To enable remedial action at the manager side

- 1 Click the **Admin** dropdown, and then click **Manager**.

- 2 In the **Configuration** tab – **Alert Events** pane, check the **Enable Remedial Action** option, if not selected by default.

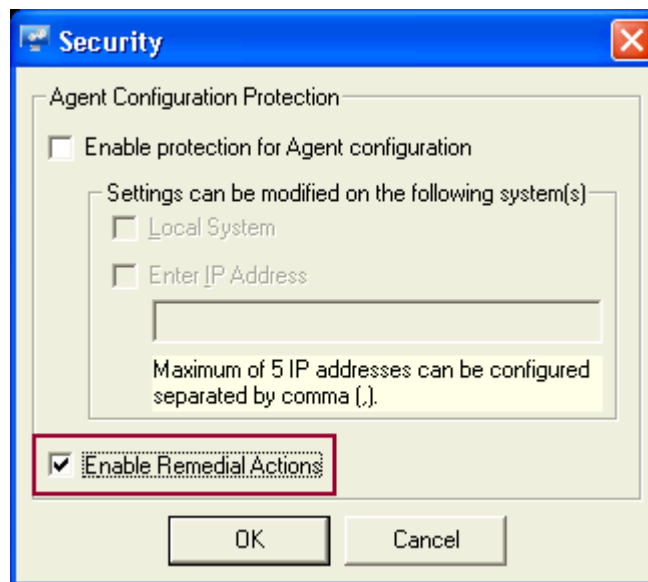
EventTracker displays the message box.



- 3 Click **OK**.
- 4 Click **Save**.

To enable remedial action at the Agent side

- 1 Open **EventTracker Control** panel.
- 2 Double-click the **EventTracker Agent Configuration**.
- 3 Select a managed system from the **Select system** drop-down list.
- 4 Click the **File** menu, and then select the **Security** option.



- 5 Select the **Remedial Action** checkbox.
 - 6 Click **OK**.
 - 7 Click **Save**.
-

Chapter 11

Configuring Event Filters

In this chapter, you will learn how to:

- [Configure Event Filters](#)
- [Configure Event Filters with exception](#)

Filtering Events from View

Fine grain filtering for meaningful monitoring support for both view and source filters based on wildcard matches of id, type, source, user, event description.

- Filter non-essential events – collect and manage only important events – minimum traffic.
- Filter any event(s) for display only (these are still logged into the event database).
- Monitor only specific events. Example – Log all events into the database but display only Audit Failure.

Create a separate monitoring window for Exchange Server events.

- Filter any specific category of events – Example,
Monitor all events except information events.
- Exclusive filters according to your own criteria – Examples,
Filter all Information events except defined list.

A few specific events are frequently generated but you wish to exclude these and monitor all other events.

- BOOLEAN operators in filter policy definitions – provides the ability to match multiple strings in fields to create sophisticated filter policy definition.

Configuring Event Filters

This option enables you to filter events of minor significance from the view.

To configure event filters

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** dropdown, and then click **Event Filters**.
EventTracker displays the **Event Filters** page.

3 Click **Add Filter**.

EventTracker displays the **Event Filter Configuration** page.

Event filter configuration

Filter Name: All Error Events with Event ID 8

Description: ☐ Active

Check to activate event filter

Filter Detail | Filter Exception | Systems

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
Application	Audit Success	0					

Add Edit Delete

Finish Cancel

4 Type the name of the filter in the **Filter Name** field.

5 Type a brief description in the **Description** field.

6 By default, EventTracker selects the **Active** checkbox. Uncheck the checkbox to deactivate the filter.

EventTracker retains the configuration settings. You can again activate the event filter by checking the "active" checkbox.

7 In **Event Filter Configuration** page, click **Add**.

8 In **Add Event** dialog box, enter/select appropriately in the relevant fields.

NOTE

If you leave a field blank, EventTracker assumes a wildcard match for that field. For example, leaving the user field blank implies that any value in that field is acceptable.

9 Click **Add**.

EventTracker displays the 'Event Filter Configuration' page with newly added filter details.

10 Click the **Systems** tab.

All Systems option is selected by default, which means the filter is applied to all the monitored systems.

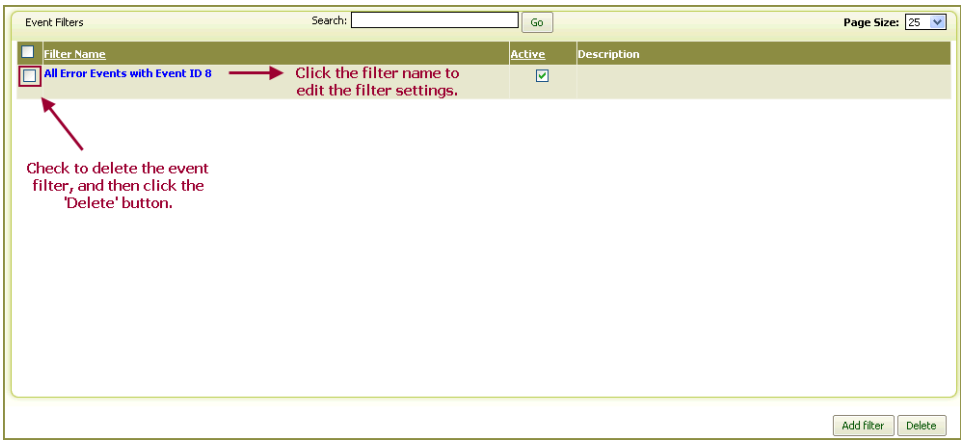
11 Select required system groups / systems to apply the filter.

12 Click **Finish**.

EventTracker displays the Event Filters page with newly added event filter.

Click the filter name to edit the filter settings.

Click the checkbox against the event filter name and then click the **Delete** button to delete the Event Filter.



Configure Event Filters with Exception

This option enables you to filter events with an exception.

To configure event filters with exception

- 1 On the **Event Filters** page, click the name of the Event Filter.
EventTracker displays the **Event Filter Configuration** page.
- 2 Click the **Filter Exception** tab.
- 3 Click **Add** to add filter exception criteria.
- 4 Enter/select appropriately in the relevant fields, and then click **Add**.
EventTracker displays the **Filter Exception** tab with newly added filter exception.
- 5 Click the **Finish** button to save the changes.

NOTE

For example, if you wish to filter out all events of **Event Type- Information** but interested in monitoring a particular event for example – Event ID 3223. Then in this case, all events of 'Information' event type will be filtered out but with one exception of event 3223.

Understanding Filters and Filter Exceptions

This section helps you understand how filters and filter exceptions work.

To understand Filters and Filter Exceptions

- 1 Click the name of the event filter.
- 2 In the **Filter Detail** tab, select the filter rule to be deleted, and then click the **Delete** button.
EventTracker displays the confirmation message box.
- 3 Click **OK** to remove the filter details.
EventTracker removes the filter details.
- 4 Click the **Filter Exception** tab.
The filter exception you have set earlier remains unaltered.
- 5 Select the exception rule to be deleted, and then click the **Delete** button.
EventTracker displays the confirmation message box.
- 6 Click **OK** to remove filter exceptions.
EventTracker removes the selected filter exception.

 NOTE

It is obvious from the above scenario; it is your responsibility to manage Filters and Filter Exceptions. The table given below will provide you a clear idea how the combination of Filters and Filter Exceptions work.

Table 73

Filter	Filter Exception	Result
Y	N	EventTracker filters all events from the view.
N	Y	EventTracker allows all events.
Y	Y	EventTracker allows events with exception.
N	N	EventTracker allows all events.

Chapter 12

Configuring Reports Settings

In this chapter, you will learn how to:

- [Configure Published Reports/Analysis Settings](#)
- [Configure Cost Saving Analysis Settings](#)

Configuring Published Reports Settings

This option helps to configure published reports settings.

To configure published reports settings

- Click the **Admin** dropdown, and then click **Report Settings**.
EventTracker displays the **Published Reports** tab.

Figure 204
Published Reports

Report Settings

Published Reports

Cost Saving Report

Reports backup directory:

Note: on changing the folder, reports have to be manually copied from older to newer folder

Folder to keep the copies of generated reports

C:\Program Files\Prism Microsystems\EventTracker\Reports

Browse...

☒ Generate Default Report in case of no matching record found

Reports purge frequency:

Note: Uncheck the options to retain reports forever. An event will be logged 2 days before file deletion, which can be viewed in the EventTracker Management console.

☒ Retain on demand/queued report for

7

 days

☒ Retain scheduled reports for

90

 days

☒ Prompt to publish on demand Quick View reports

On demand 'Quick view' reports are not published on hard disk This option will prompt to publish the report before closing.

☐ Replace Domain/User fields from the Event Description if found.

DNS Custom Column Resolution Url:

http://whois.domaintools.com/IP-ADDRESS

Report Header

EventTracker

Report Footer

Reports

Ok

Cancel

Table 74

Field	Description
Reports backup directory	Folder to keep copies of generated reports. By default, EventTracker saves the reports in ...\\Program Files\\Prism Microsystems\\EventTracker\\Reports folder. You can select a different folder as you wish. On changing the folder, manually copy the reports from old to new folder
Generate Default Report in case of no matching record found	If checked, EventTracker will generate a PDF with the message "No Matching Record Found," if there are no matching records found for the Queued or Scheduled reports. The PDF will be generated irrespective of the report format type.
Reports purge frequency	Time schedule for the reporter to remove saved 'On Demand/Queued' and 'Scheduled' reports from the hard disk. EventTracker raises an event (2029) two days prior to deletion. EventTracker displays those events under the All Categories -> EventTracker -> EventTracker: Published reports cleanup Category. Clear the checkboxes to retain all the reports forever. By default, Reporter will retain 'On Demand/Queued' and 'Scheduled' reports for 7 and 90 days respectively.

Field	Description
Prompt to publish on demand Quick View repots	On demand "Quick view" reports are by default not published/saved on hard disk. Selecting this option will prompt you with an option to save/publish the report before closing.
Replace Domain/User fields from the Event Description if found	<p>By default, EventTracker looks for the following keywords</p> <p>Keywords for Domain: Client Domain/ Domain/ User ID/ Account Domain (2nd Instance)</p> <p>Keywords for User: Client User Name/ Target Account ID/ User Name/ Account Name (2nd Instance)</p> <p>Advanced Reports looks for these keywords in event description. If corresponding key-value is not blank then it will overwrite the original domain/user field with key-value in the display.</p> <p>E.g. Event Domain is NT AUTHORITY. In Event Description Client Domain is TOONS. It will display TOONS instead of NT AUTHORITY</p> <p>If this checkbox is cleared, then EventTracker displays the original domain/user.</p>
DNS Custom Column Resolution Url	URL to resolve IP address.
Report Header	Specify a header for the published reports.
Report Footer	Specify a header for the published reports.

Table 75

Event Id	Description
2029	<p>Source: EventTracker</p> <p>Description Notification: Report file deletion</p> <p>Following file Logs - created on will be deleted on so, please take back up of the file if required.</p> <p>Event Information Cause :</p> <p>This event is logged when EventTracker On Demand and Schedule reports start purging the published files.</p>

Configure Cost Saving Reports Settings

Figure 205
Cost saving analysis

- Click the **Cost Saving Analysis** tab.

Report Settings

Published Reports

Cost Saving Report

Cost Saving Analysis

Time (Seconds) taken for manual analysis - These settings show the time required to perform each of the functions manually. When performed automatically by EventTracker, this is the time saved. These values are used to compute overall time/cost savings.

Analyst - These settings show the person who will be analyzing the events.

Cost of Manual Analysis

		Time (Seconds) taken for manual analysis	Analyst
Edit	Events analyzed	0.05	Senior IT Admin
Edit	Alerts raised	1	Senior IT Admin
Edit	Systems monitored	2	Senior IT Admin
Edit	Specialized events	0.5	Senior IT Admin

Labor Rate[Cost/Hour]

Junior IT Administrator

26

Currency Type

USD

Senior IT Administrator

40

Note: **Labor rate shows the total cost per hour of a system administrator's time. These values are used to compute total cost savings.

Ok

Cancel

- Click **Edit** to modify the **Time (Seconds) taken for manual analysis** and **Analyst** field.

Labor rates [Cost/Hour] - Shows the fully loaded labor cost per hour of a system administrator's time. These values are used to compute total cost savings.

Currency Type – Labor cost will be displayed in the selected currency.

NOTE

Before generating any cost saving analysis, please make sure that **Collect cost savings information** checkbox is enabled in **Manager >>Configuration.(Cost Saving Report)**

Chapter 13

Analyzing Logs

In this chapter, you will learn how to:

- [Reg-ex Help](#)
- [Analyze Logs](#)
- [Analyze Alerts](#)
- [Analyze Log Volume](#)
- [Analyze Suspicious Traffic](#)
- [Analyze ROI](#)

Reg-Ex Help

This option allows you to query using regular expressions. Complex expressions can take longer. Use the 'Wizard' hyperlink to build the regular expression string used in the "Match for specific information" and "Filter specific information" fields.

How to Create a New Group

- 1 Log on to **EventTracker Enterprise**.
- 2 Move the mouse pointer over **Reports** menu and then select **Flex reports**.
OR
- 3 Click the **Reports** menu, and then click **Flex reports** tab.
- 4 In **Flex Report** pane, expand **Logs**.
- 5 Right click **Summary/ Detail/ Trend**, and then select report type from **On Demand/ Queued / Scheduled / Defined**.
- 6 Select required category or events properties, and then click **Next >>**.
- 7 Select the required or **Groups/ System/ All Systems** for the report, and then click **Next >>**.
- 8 Select the time duration and formatting options for the report, and then click **Next >>**.
- 9 In the **Refine** and **Filter** criteria page, click the **Advanced** option.

Figure 206
Refine and Filter
page

Regular expression based query can be formed only while generating Flex Report >> Logs.

Refine and Filter Page

☐ Basic (Direct query)
 ☒ Advanced (Regular expression based query)
 [Wizard](#)

<p>Refine</p> <p>Match for User(s):</p> <div style="border: 1px solid gray; height: 20px; width: 100%;"></div> <p>Match for specific information:</p> <div style="border: 1px solid gray; height: 50px; width: 100%;"></div>	<p>Filter</p> <p>Filter User(s):</p> <div style="border: 1px solid gray; height: 20px; width: 100%;"></div> <p>Filter specific information:</p> <div style="border: 1px solid gray; height: 50px; width: 100%;"></div>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Filter Event Id(s):

Filter Event Source(s):

Notes:

Use this option to query using regular expressions. Complex expressions can take longer.

Use the "Wizard" to build the regular expression string used in the "Match for specific information" and "Filter specific information" fields

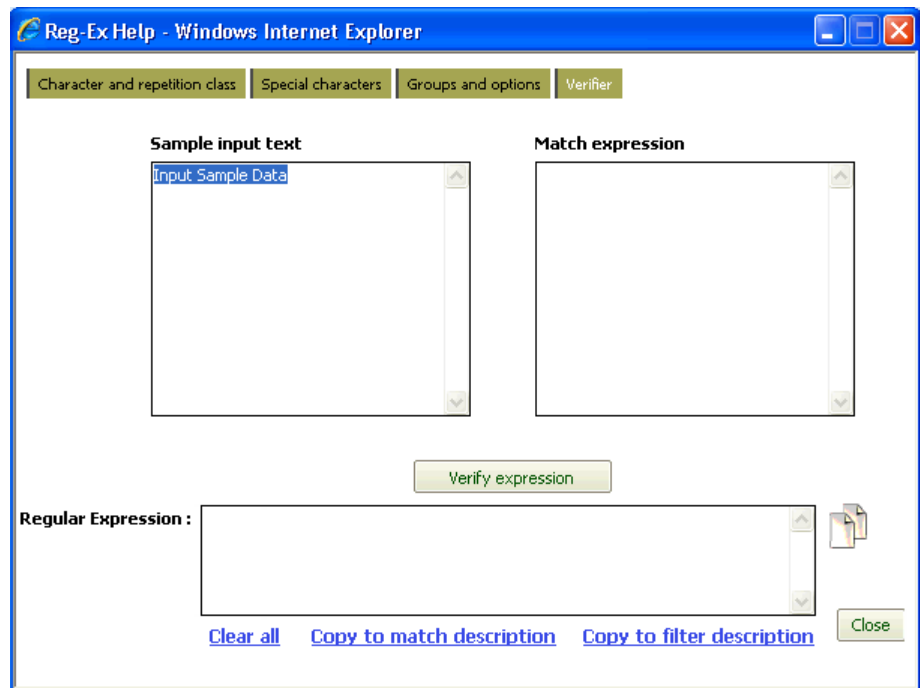
- 10 Click the **Wizard** hyperlink.

Figure 207
Reg-Ex Help window

Form a suitable
Regular Expression
to be searched in the
description by
selecting the wildcard
characters in the
respective tabs.

- 11 From the "Character and Repetition class", "Special Characters", and "Groups and Options" tabs, select required regular expressions.
- 12 Type the expression you want to search in the **Regular Expression** field.
- 13 Click the **Verifier** tab.

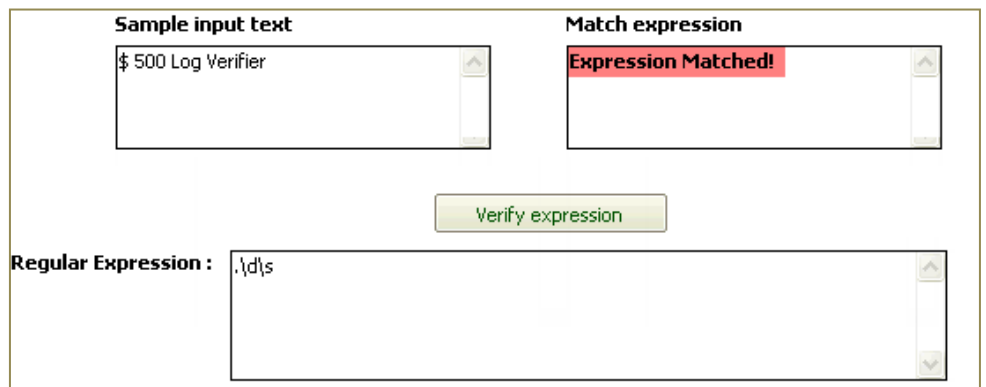
Figure 208
Reg-Ex Help window



14 In the **Sample Input** field, type a sample text to verify the correctness of the selected regular expression.

15 Click **Verify Expression**.

EventTracker displays 'Expression Matched' message if the sample text matches to the provided regular expression.



On the other hand, if the sample text does not match to the provided regular expression then EventTracker displays 'Expression not Matched' message.



The screenshot shows a web interface with three main sections. At the top left, a box labeled 'Sample input text' contains the text '\$ 500 Log Verifier'. To its right, a box labeled 'Match expression' contains the text 'Expression Not Matched!'. Below these two boxes is a green button labeled 'Verify expression'. At the bottom, a box labeled 'Regular Expression :' contains the text '.\d\s'.

16 Click  to copy the **Regular Expression** to the clipboard.

17 Click **Copy to match description** or **Copy to filter description** hyperlink.

EventTracker copies the text to **Match for specific information/ Filter specific information** fields in the **Refine** and **Filter** criteria page

About Parsing Rule

To be precise, parsing rules are user-defined tokens. Apart from the standard report definition format, EventTracker reports module provides a simple, yet powerful log Flex Reports, reporting facility.

It helps to parse and include parts of clogged syslog like messages and Windows event descriptions as columns in reports.

Parsing rule helps you define new tokens, bind it with the dynamic report templates and generate flex reports. EventTracker displays the parsed data under those tokens defined by you.

While configuring Flex reports, you can also select the report columns you are interested in, apply filters, sort report columns, and rearrange the order of the columns that should appear in reports.

To put it in a nutshell **Parsing rule** helps to manipulate data and generate comprehensible reports.

The Need for Adding Parsing Rule in Flex Report

Scouring the components of log data is massively time. Data contains pieces of information.

Since valuable information is dumped in the log description, there should be a way to break down and analyze the data, and turn it into valuable business information.

Furthermore, there is no standardized message format as various vendors of NIX systems follow different conventions.

For example, comma-separates values, fixed-width text, and free-form text. administrator to decipher sys log messages.

How EventTracker Helps?

A common questions that arises would be,

- 'Is it not sufficient to generate **Flex reports** with templates provided with EventTracker?"
- Is EventTracker flexible enough to add tokens?
- If so, does not EventTracker provide any predefined tokens to simplify my work?
- Is it possible to define my own tokens?

If you're preoccupied with these questions, relax!

EventTracker is shipped along with a precisely defined set of tokens for your convenience. Should you wish to add tokens if these predefined tokens do not align with your requirement, EventTracker provides adequate facilities to add/modify/delete tokens. Otherwise, default tokens are sufficient.

IF I BIND NEW TOKEN-VALUE TO THE PARSING RULE, WILL THOSE TOKEN-VALUE BE SAVED PERMANENTLY IN THE DATABASE?

It's left to your discretion. While defining new Token-Value, you have the luxury of saving the Token-Values permanently in the database or binding the Token-Value just for one instance of report generation.

Prior Knowledge

It is appreciable to have comfortable knowledge and understanding of syslog message formats of different flavors of NIX systems. Though the fundamental tenets insist on simplicity, the creators of syslog write the messages according to their whim and caprice. So suit yourself to the environment you work in to understand the syntax and semantics of syslog messages.

Components of Parsing Rules

Components of **Parsing rules** are the basic elements that are essential in framing your queries to extract required data from the log messages.

What is Token?

Token is the 'key' that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide token and can contain:

- Characters (a, b, c...)

- Numbers (1, 2, 3...)
- Special characters (#, \$, %), space character...
- or combination of all three (a1#)

Parsing Rule Occurrences

If there are multiple occurrences of token in the description, reporter engine considers only the first occurrence as reference point. So, be specific while you frame your query.

What is Display Name?

Display Name is a temporarily assumed name (alias) for the queried string. This name will appear as token in the report. It is mandatory to provide display name and should be unique throughout the report. You can select any name and can contain:

- characters
- numbers
- or combination of these two
- special characters are not accepted

What is Separator?

Separator is a character or word which separates key and value in the description. It is optional to provide separator and can contain:

- characters
- numbers
- special characters
- or combination of all three

What is Terminator?

Terminator is character or word to determine end of key value pair in description. The queried string is extracted till the first occurrence of the terminator. It is optional to provide terminator and can contain:

- Characters
- Numbers
- Special characters
- or combination of all three

Thus, parsing rule offers flexibility to customize:

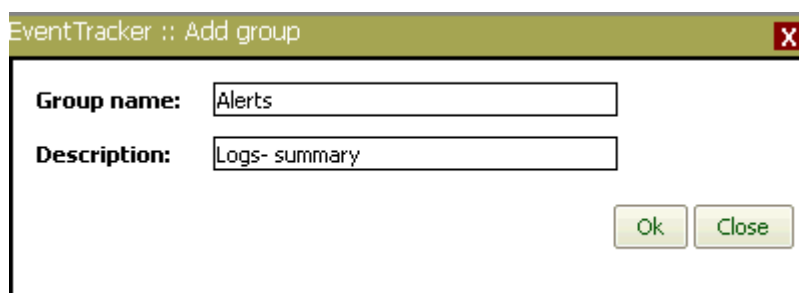
- Data selection

- Sort sequences

To Add group

- 1 Right click Flex reports and select New Group
- 2 EventTracker displays Add Group window
- 3 Fill in the **Group name** and **Description** and click **OK**.

Ex: Create a new group name as SCAP and description as Logs click OK



A new group Alerts is created under the Flex Reports pane.

Right click newly created group to **Edit** or **Delete** the group

Note:

The new group can be deleted only when the group does contain any reports

Logs - Summary
Step 4 of 9

Select duration for the report.

Interval

☒ **Select interval:**

Last 1 Day

▼

☐ **Select date range:**

From :

10/4/2012

05 : 46 : 04 : PM

+

-

[mm/dd/yyyy]

[hh:mm:ss]

To :

10/4/2012

06 : 46 : 04 : PM

+

-

☐ **Limit to time range**

More options

Format option:

Summary

▼

☐ **Standard rule**

☒ **Parsing rule**

☐ **Token template**

Export type:

Quick view (not saved on hard disk)

▼

Cancel

<< Back

Next >>

EventTracker provides predefined parsing rule that can be chosen from the select Parsing Rule wizard.

Logs - Summary
Step 5 of 9

Select or add rule(s) to display

Select Parsing Rule

☐ **Display name**

☐ Log Time

☐ Event Id

☐ Event User

☐ Computer

☐ Event Source

☐ Event Description

Token

Log Time

Event Id

Event User

Computer

Event Source

Event Description

Separator

Terminator

Resolution

Remove

EventTracker displays list of predefined parsing rule to select from,

<input type="checkbox"/>	Display name	Token	Separator	Terminator	Resolution	Group
<input type="checkbox"/>						
<input type="checkbox"/>	Accesses	Accesses	:	\n		Default
<input type="checkbox"/>	Authentication Type	Authentication Type	:	\n		Default
<input type="checkbox"/>	Caller Process ID	Caller Process ID	:	\n		Default
<input type="checkbox"/>	Client Domain	Client Domain	:	\n		Default
<input type="checkbox"/>	Client User Name	Client User Name	:	\n		Default
<input type="checkbox"/>	Error Code	Error Code	:	\n		Default
<input type="checkbox"/>	File Object Name	File Object Name	:	\n		Default
<input type="checkbox"/>	Image File Name	Image File Name	:	\n		Default
<input type="checkbox"/>	Logon Account	Logon Account	:	\n		Default
<input type="checkbox"/>	Logon GUID	Logon GUID	:	\n		Default
<input type="checkbox"/>	Logon ID	Logon ID	:	\n		Default

OkClose

Logs - Summary

Step 5 of 9

Select or add rule(s) to display

Select Parsing Rule

Help

<input type="checkbox"/>	Display name	Token	Separator	Terminator	Resolution
<input type="checkbox"/>	Log Time	Log Time			
<input type="checkbox"/>	Event Id	Event Id			
<input checked="" type="checkbox"/>	Event User	Event User			
<input type="checkbox"/>	Computer	Computer			
<input type="checkbox"/>	Event Source	Event Source			
<input type="checkbox"/>	Event Description	Event Description			

Remove

Summary

☐ Log Time

☐ Event Id

☒ Event User

Report columns

Sort by

Log Time

Cancel<< BackNext >>

Logs - Summary

Step 6 of 9

You can narrow down the criteria by explicitly specifying the details.

Basic (Direct query)

Advanced (Regular expression based query)

Refine

Match for User(s):

Match for specific information:

Filter

Filter User(s):

Filter specific information:

Filter Event Id(s):

Filter Event Source(s):

Notes:

Use this option for simple queries (to use regular expressions, go to "Advanced").
The 'Refine' option is inclusive. Results are limited to matching entries.
The 'Filter' option is exclusive. Results do not include matching entries.
Any combination of Refine and Filter may be used simultaneously.
Examples:
1) Match for User(s):

Cancel

<< Back

Next >>

Token templates

Parsing Rule

Template

Token-Value Groups

Default

CiscoTest

Juniper

mani

mani2

mahendra

Token-Value

Group: All

Display name	Token	Separator	Terminator	Resolution	Description
<input type="checkbox"/> Accesses	Accesses	:	\n		
<input type="checkbox"/> Accesses	Accesses2	:	\n		mani
<input type="checkbox"/> Authentication Type	Authentication Type	:	\n		
<input type="checkbox"/> Authentication Type	Authentication Type2	:	\n		
	Caller Domain	:	\r\n		
<input type="checkbox"/> Caller Process ID	Caller Process ID	:	\r\n	DNS and WHOIS	
<input type="checkbox"/> Caller User Name	Caller User Name	:	\r\n		
	Computer	:	\n		
	Event Description	:	\n		

Add Rule

Edit

Delete

Move to group

Token-Value Wizard

Analyzing Logs

Filter and display event logs based on user-defined criteria. The user can define the filter (or exclude) string as well as specify the output format.

Usage: Forensic analysis of specific events, broad searches per criteria with subsequent sorting and ordering of the result set.

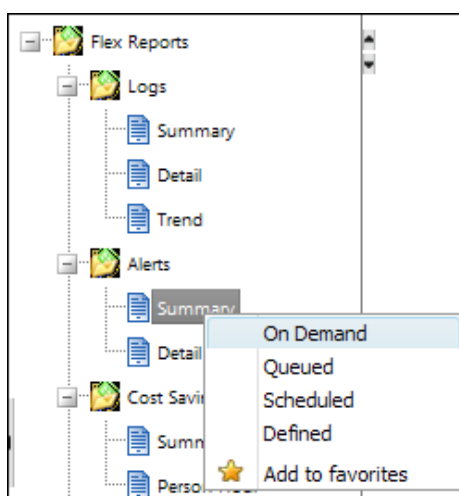
Flex Reports - Summary - On Demand

Standard Column Flex reports

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.

- 2 Click Reports and point mouse to Flex Reports.
 - 3 Expand **Logs** in the Flex report tree.
 - 4 Right-click **Summary**.
- EventTracker displays the shortcut menu.

Figure 209

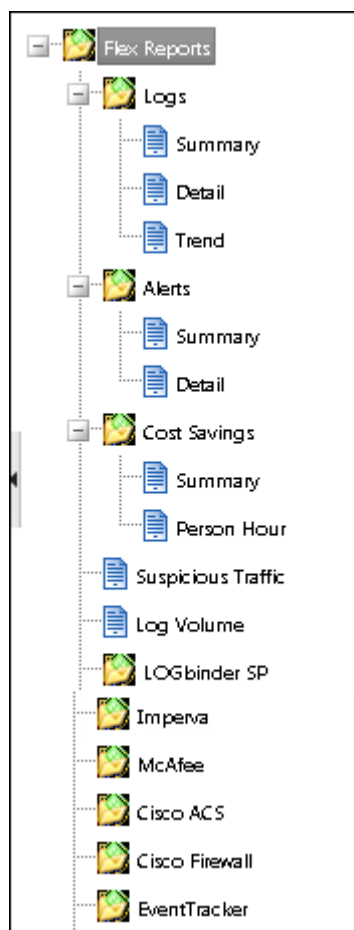


From the shortcut menu, choose **On Demand**.

(OR)

Select the **Summary** option and then click **On Demand** in the Actions pane.

Figure 210

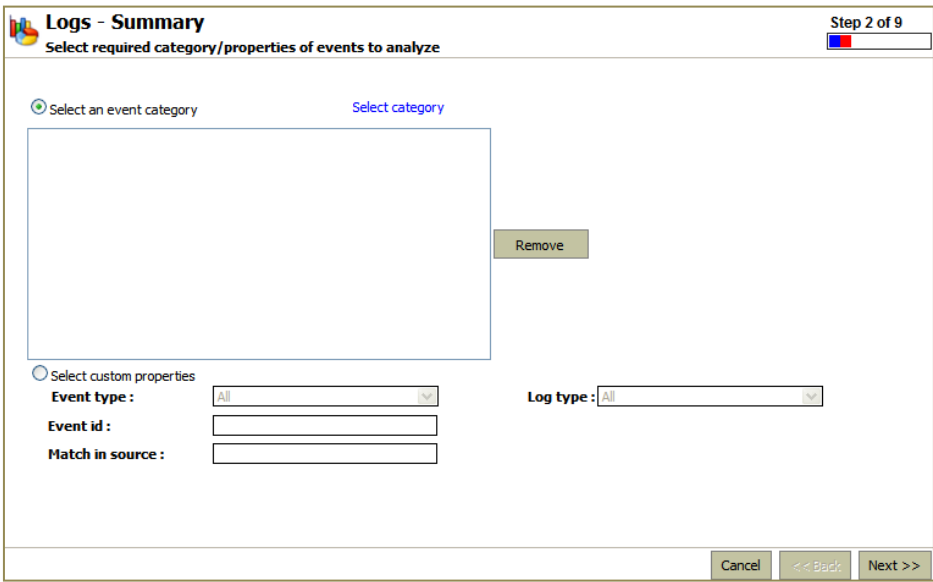


EventTracker displays the Reports Wizard.

- 5 Click **Next >>**.

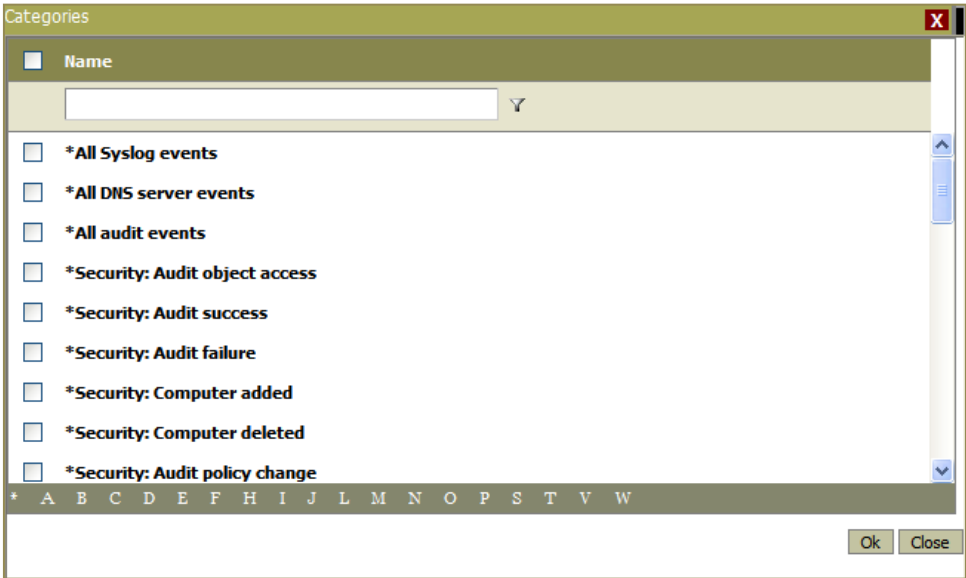
EventTracker displays the 'Select required category/properties of events to analyze' page.

Figure 211
Select
Category/Property



- Select the **Select an event category** option:
 1. Click '**Select category**' hyperlink to view all predefined categories.
EventTracker displays **Categories** pop up window.

Figure 212
Categories

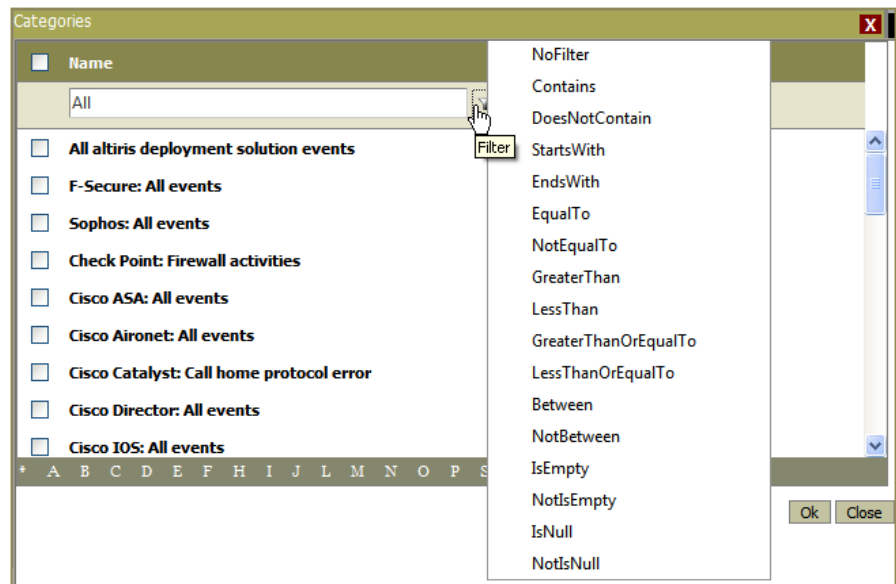



2. Select the checkbox against the required category name **OR** select the checkbox against '**Name**' to select all the categories **OR** filter the categories by alphabets given at the bottom of the categories list.

OR

Filter the categories using category name or part of category name.

Figure 213
Categories

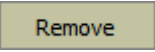


Enter the category name or part of category name in the filter box, and then click the filter  icon.

Here you can find different options to filter the given criteria.

3. Select the required option in the **Categories** window, and then click the **Ok** button.

The selected categories will appear in the '**Select an event category**' box.

NOTE: Make use of **Remove**  button to remove the categories from selection.

- Select '**Select custom properties**' option:

1. Select event type from the **Event type** dropdown list.
2. Select log type from **Log type** dropdown list.
3. Enter Event ID number in the **Event ID** field.

You can enter multiple Event IDs using separator '&&'. Example: 592 && 577 && 861

4. Enter source name in **Match in source** field.

- 6 Click **Next >>**.

EventTracker displays the '**Select system(s) or group(s) for analysis**' page.

- 7 Select the **Groups/ Systems / All systems** option, and then click the **Next** button.

EventTracker displays the '**Interval and More Options**' pane.

Figure 214
Reports duration

Select the interval for reports:

Select this option, EventTracker considers events occurred during the selected number of days for reports. Select this option and select **Limit to time range** checkbox. EventTracker enables the **From** and **To** spin boxes. Set the time range. EventTracker considers only events occurred in that time range for reports.

Select custom date range:

Select this option, EventTracker considers events occurred during the selected number of days for analysis. Select this option and select **Limit to time range** checkbox. EventTracker enables the **From** and **To** spin boxes. Set the time range. EventTracker considers only events occurred in that time range for analysis.

Note that EventTracker considers only the date range from the From, To drop-down lists and ignores the time range set in those drop-down lists.

- In Interval pane:

1. Select '**Select Interval**' option (if not selected), and then select the report generation Interval from the dropdown list.

OR

Select '**Select the Date range**' option, and select the date and time in '**From**' and '**To**' field.

2. Select '**Limit to time range**' checkbox, and then select the time limit in '**From**' and '**To**' field.

- In More options pane:

1. Select the **Format option** as **Summary**.

2. Select **Standard column** option, EventTracker displays **Sort by** dropdown list.
Select appropriate **Sort by** Option.
 3. Select the export type as 'Quick view' form **Export type** dropdown list.
- 8 Make appropriate selection, and then click the **Next** button.
- EventTracker displays 'You can narrow down the criteria by explicitly specifying the details' page.

Figure 215
Filter criteria

Logs - Summary Step 6 of 9

You can narrow down the criteria by explicitly specifying the details.

☒ Basic (Direct query) ☐ Advanced (Regular expression based query)

Refine	Filter
Match for User(s):	Filter User(s):
Match for specific information:	Filter specific information:
Filter Event Id(s):	
Filter Event Source(s):	

Notes:

Use this option for simple queries (to use regular expressions, go to "Advanced").
The 'Refine' option is inclusive. Results are limited to matching entries.
The 'Filter' option is exclusive. Results do not include matching entries.
Any combination of Refine and Filter may be used simultaneously.

Examples:

1) Match for User(s):

Cancel << Back Next >>

- 9 Click the **Basic/ Advanced** option.
- Select **Basic (Direct Query)** option:
1. Enter the **Refine** and **Filter** criteria.
 2. Enter **Filter Event ID(s)** and **Event Source(s)** to be filtered out from the report.
- You can type either Event ID(s) or Event Source(s) or both. All are optional values.

OR

Select **Advanced (Regular expression based query)** option

Figure 216
Select Advanced
option

☐ Basic (Direct query)
 ☒ Advanced (Regular expression based query) [Wizard](#)

Refine	Filter
Match for User(s): <input type="text"/>	Filter User(s): <input type="text"/>
Match for specific information: <div><input type="text"/></div>	Filter specific information: <div><input type="text"/></div>
Filter Event Id(s): <input type="text"/>	
Filter Event Source(s): <input type="text"/>	

EventTracker disables Match for User(s) and Filter User(s) fields. You can construct query to Match for specific information or Filter specific information.

1. Click **Advanced (Regular expression based query)** option, and then click the **Wizard** hyperlink.
2. EventTracker displays **Reg-Ex Help** wizard.
Please refer [Reg-Ex Help](#) section for more details.
- 10 Click the **Next>>** button.
EventTracker displays '**Provide title and description**' page.
- 11 Type the Title, Header, Footer, and Description, and then click the **Next** button.
EventTracker displays '**Review cost details and configure the publishing options**' page.
- 12 Crosscheck the **Disk cost analysis** details.
- 13 Select **Add to Queue** checkbox, to process the report at a later point in time.
Update status via RSS field gets enabled.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**.
- 14 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 15 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 16 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**.
- 17 Click the **Next** button.
EventTracker displays '**Review all the configuration details before submitting the Flex Reports request**' page.

18 Crosscheck the **parameters**, and then click the **Generate** button.

Quick View (Smart Viewer)

Smart Viewer allows you to subtly refine the intricate result set with ease. Initially Smart Viewer displays the Summary, Extended Summary and then the Detailed view. Presently supports On Demand Category based reports (Summary & Extended Summary) and Log Flex Reports(Summary) based on Event Categories and Custom Properties.

Note



Add to queue (background processing), **Enable publishing option**, **Show in** (Compliance Dashboard) and **Updated status via RSS** options will not available if you select Quick View as Export type.

- Click a record to view the Extended Summary.
 - Click a record to view details and refine the result set.
 - Click the hyperlink in the **Event Id** column to view the event details in EventTracker Knowledge Base.
-

Custom Column Flex Reports

- 1 Select **Summary** in the Flex Reports.
- 2 Click **On Demand** in the Actions pane.
- 3 Click **Next >>**.
- 4 Select the **Select custom properties** option, type appropriately in the relevant fields, and then click **Next**.
- 5 Select the Groups / Systems / All Systems, and then click **Next**.
- 6 Select the report generation Interval.
- 7 Select the **Format option** as **Summary**.
- 8 Select the Export type, and then click the **Next** button.

Note



Export type can be of any type and need not be Excel. Custom columns will be displayed as Row summary information and not as column in the report as done in the case of detail report.

EventTracker displays the '**Select or add Column(s) to display**' page.

- 9 Click **Add New Column** button.
- 10 Enter the **Display name** and **Column name**.
- 11 Select **Add to select column** checkbox to add new columns to selected columns list.
- 12 Select **Save this column key** checkbox to save the new column names into the database.
- 13 Click the **Add** button.
EventTracker adds custom column.
- 14 In **Summary** and **Report Columns** field, click the up/down arrow keys to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.
Select the required report column, and then click up/down arrow to move the column.
- 15 Select the **Sort by** option and then click **Next>>**.
- 16 Type the **Refine** and **Filter** criteria.
- 17 Type the Title, Header, Footer, and Description.
- 18 Crosscheck the **Disk cost analysis** details.
- 19 Select **Add to Queue** checkbox, to process the report at a later point in time.
EventTracker enables the **Enable publishing option** checkbox and **Update status via RSS** drop-down list.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**
- 20 Enter Email ID in **To E-mail** box to deliver/notify the results via emails.
- 21 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 22 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to be shown in Compliance Dashboard.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**.
- 23 Crosscheck the **Report parameters**.
- 24 Click **Generate**.

Note



You can also exclude predefined columns from the report. EventTracker does not save this exclusion in the database.

Flex Reports - Detail - On Demand

Standard Column Flex Reports

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex Report**
- 3 Expand **Logs** in the Flex Reports tree.
EventTracker displays the Logs page.

Note

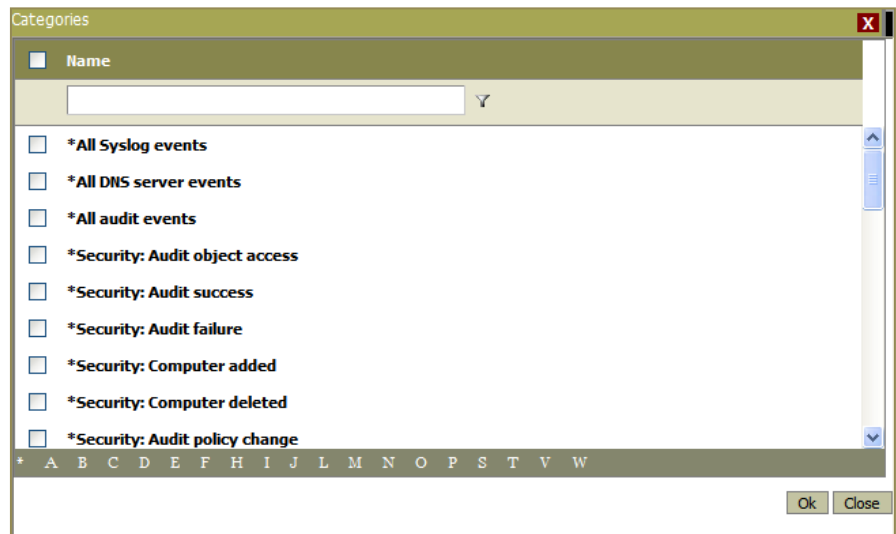


If there are no generated analyses, then EventTracker displays the page with empty panes.

You can define or schedule reports/analyses with the same configuration settings of generated reports/analyses. To do this, select a generated report in the top pane, select an appropriate option from the **Use Configuration** drop-down list and then click **Go**. EventTracker starts the Reports Wizard.

- 4 Right-click **Detail**.
EventTracker displays the shortcut menu.
From the shortcut menu, choose **On Demand**.
(OR)
Select the **Detail** option and then click **On Demand** in the Actions pane.
EventTracker displays the Reports Wizard.
- 5 Click **Next >>**.
EventTracker displays the '**Select required category/properties of events to analyze**' page.
 - Select the **Select an event category** option:
 1. Click '**Select category**' hyperlink to view all predefined categories.
EventTracker displays **Categories** pop up window.

Figure 217
Categories

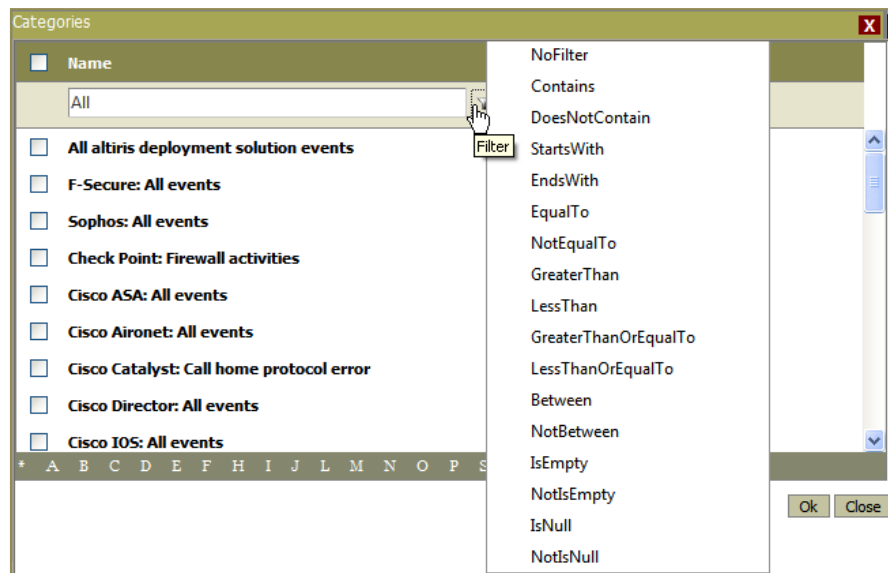



2. Select the checkbox against the required category name **OR** select the checkbox against '**Name**' to select all the categories **OR** filter the categories by alphabets given at the bottom of the categories list.

(OR)

Filter the categories using category name or part of category name.

Figure 218
Categories

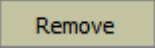


Enter the category name or part of category name in the filter box, and then click the filter  icon.

Here you can find different options to filter the given criteria.

3. Select the required option in the **Categories** window, and then click the **Ok** button.

The selected categories will appear in the '**Select an event category**' box.

NOTE: Make use of **Remove**  button to remove the categories from selection.

- Select '**Select custom properties**' option:

1. Select event type from the **Event type** dropdown list.
2. Select log type from **Log type** dropdown list.
3. Enter Event ID number in the **Event ID** field.

You can enter multiple Event IDs using separator '&&'. Example: 592 && 577 && 861

4. Enter source name in **Match in source** field.

- 6 Click **Next >>**.

EventTracker displays the monitored Groups and Systems page.

- 7 Select the Groups / Systems / All Systems, and then click **Next>>**.

EventTracker displays the 'Interval and More Options' pane.

- 8 Select the report generation Interval.
- 9 Select the **Limit to time range** checkbox, to set the time range limit.
- 10 Select the **Format option** as **Detail**.
- 11 Select the **Export type**.
- 12 Select the **Sort by** option.
- 13 Type the **Refine** and **Filter** criteria.

Table 76

Field	Description
Basic Search	<p>Use this option for simple queries (to use regular expressions, go to "Advanced").</p> <p>The 'Refine' option is inclusive. Results are limited to matching entries.</p> <p>The 'Filter' option is exclusive. Results do not include matching entries.</p> <p>Any combination of Refine and Filter may be used simultaneously.</p> <p>Examples:</p> <p>Match for User(s):</p> <p>Enter usernames separated by (for OR)</p> <p>The entry 'bruce peter clark' for a Login failure report will show results for only those usernames.</p> <p>Match for specific information:</p> <p>Enter multiple strings separated by && (for AND) or (for OR)</p> <p>Special characters (" , ^, \$) must be preceded by '\'</p> <p>The entry 'FLR1PRINTER' for a Printer Usage report will limit results to that printer.</p> <p>The entry 'bruce' in Match for Users and 'FLR1PRINTER' in Match for specific information may be specified.</p> <p>The entry 'FLR1PRINTER&&budget.xls' in Match for specific info shows all matching entries.</p>
Advanced Search	<p>Use this option to query using regular expressions. Complex expressions can take longer.</p> <p>"Use the Wizard" to build the regular expression string used in the "Match for specific information" and "Filter specific information" fields.</p>

14 Select the **Basic/Advanced** option.

Select **Basic (Direct Query)** option:

1. Enter the **Refine** and **Filter** criteria.
2. Enter **Filter Event ID(s)** and **Event Source(s)** to be filtered out from the report.

You can type either Event ID(s) or Event Source(s) or both. All are optional values.

OR

Select **Advanced (Regular expression based query)** option:

EventTracker disables **Match for User(s)** and **Filter User(s)** fields.

You can construct query to **Match for specific information** or **Filter specific information**.

1. Click **Advanced** option, and then click the **Wizard** hyperlink.
2. EventTracker displays **Reg-Ex Help** wizard.

Please refer [Reg-Ex Help](#) section for more details.

- 15 Type the Title, Header, Footer, and Description, and then click the **Next** button.

EventTracker displays '**Review cost details and configure the publishing options**' page.

- 16 Crosscheck the **Disk cost analysis** details.

- 17 Select **Add to Queue** checkbox, to process the report at a later point in time.

Update status via RSS field gets enabled.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 18 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.

- 19 Select RSS Feed from the Update status via RSS to get RSS notification.

- 20 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 21 Click the **Next** button.

EventTracker displays '**Review all the configuration details before submitting the Flex Reports request**' page.

- 22 Crosscheck the **Reports parameters**, and then click the **Generate** button.
-

Quick View

Quick View allows you to refine the result set. Quick View reports are not stored in the hard disk; you have to explicitly export those reports. Click the **Export** icon on the top strip to export the report. The exported reports can also be viewed in the Dashboard.

Note



Add to Queue (background processing), **Enable publishing option**, **Show in** (Compliance Dashboard), and **Updated Status via RSS** options will not be available if you select Quick View as Export type.

Custom Column Flex Reports

- 1 Click **On Demand** in the Actions pane.
- 2 Click **Next >>**.
- 3 Select the **Select custom properties** option, type appropriately in the relevant fields, and then click **Next>>**.
- 4 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 5 Select the report generation Interval.
- 6 Select the **Format option** as **Detail**.
- 7 Select the **Custom column** option.
EventTracker selects the **Export Type** as Excel File.
- 8 Click **Next>>**
EventTracker displays the '**Select or add Column(s) to display**' page.

SELECT 'DEFAULT' OPTION:

1. Select the checkbox against the **Column Name** to add in Report.
You can also add custom columns. Click **Add New Column** to add custom columns.

Table 77

Field	Description
Display name	Type the alias of the column in this field. This could be any name and it is mandatory. Accepts characters and numbers excluding special characters.
Column name	Type the name of the column in this field. Accepts any character and numbers including special characters.

Add to selected columns	This is a shortcut to add the new columns to Selected Columns list. Type a column name and then click Add . EventTracker does not save the new column names into the database.
Save this column key	This is a shortcut to add the new columns to the Selected Columns list and EventTracker saves the new column names into the database. Type a column name and then click Add .
Report Columns	EventTracker includes the columns that are selected in the report. You can also arrange the order of the columns that should appear in the report by selecting the columns and then by clicking the arrow keys.
Summary	Select the checkboxes against the report columns. These columns are included in the summary of the report. Event Description, Event Id, and Log Time cannot be included in the summary.
Sort by	Select an appropriate option of the sort order from this drop-down list.

2. EventTracker displays the selected columns in the **Report columns** field.
3. Set the order of the columns that you want to display in the report by selecting columns in **Report Columns** and clicking arrow buttons.
4. Select the **Sort by** option and then click **Next>>**.

SELECT 'ADVANCED' OPTION:

Separator is a character that separates the key and its value. Terminator is a character that concludes the key.

Separator and Terminator feature facilitates you to query and highlight parts of clogged Syslog like messages, as columns in reports. Since there is no standardized message format and different conventions are being followed by vendors of NIX systems, it is difficult even for a seasoned user to decipher Syslog messages. Being said that, it is expected to have familiarity with Syslog message formats of different flavors of NIX systems.

By default, Windows separator is a colon (:) and terminator is a new line character (\n).

Table 78

Field	Description
-------	-------------

Display name	Type the alias of the column in this field. This could be any name and it is mandatory. Accepts characters and numbers excluding special characters.
Column name	Type the name of the column in this field. Accepts any character and numbers including special characters.
Add to selected column	This is a shortcut to add the new columns to Selected Columns list. Enter a column name and then click Add. EventTracker does not save the new column names into the database.
Separator	Type the separator character. Accepts any character and numbers including special characters.
Terminator	Type the terminator character. Accepts any character and numbers including special characters.
Resolution	<p>Resolution drop-down list is enabled only when the Advanced option is selected.</p> <p>This option helps to resolve IP address of the host by doing DNS lookup and view event & port details in the EventTracker Knowledge Base.</p> <p>EventTracker adds hyperlinks in the generated report that enables you to navigate to the EventTracker Knowledge Base Web site to get more information on Events and ports and DNS look up Web site to resolve IP address.</p>
Report Columns	EventTracker includes the columns that are selected in the report. You can also arrange the order of the columns that should appear in the report by selecting the columns and then by clicking the arrow keys.
Summary	Select the checkboxes against the columns. These columns are included in the summary of the report. Event Description, Event Id, and Log Time cannot be included in the summary.
Sort by	Select an appropriate option of the sort order from this drop-down list.

Table 79

Field	Description
-------	-------------

Add New Column	Add the column name to the Available Columns list. You have to explicitly click Add > to add those columns to the Selected Columns list.
Add to selected columns	This is a shortcut to add the new columns to Selected Columns list. Type a column name and then click Add . EventTracker does not save the new column names into the database.
Save this column key	This is a shortcut to add the new columns to the Selected Columns list and EventTracker saves the new column names into the database. Type a column name and then click Add .

Table 80

Field	Description
Edit	Select a row, select the checkbox at the right hand side and then click Edit to modify the selected row. EventTracker displays the Separator and Terminator fields. Modify appropriately and then click Update .
Delete	Select a row, select the checkbox at the right hand side and then click Delete to delete the selected row.

1. Select the checkboxes against the predefined **Column Name(s)** to add in Report.
You can also add custom columns. Click **Add New Column** to add custom columns.
 2. EventTracker displays the selected columns in the **Report Columns** field.
 3. Set the order of the columns that you want to display in the report by selecting columns in **Report Columns** and clicking arrow buttons.
 4. Select the **Sort by** option.
- 9 Click **Next>>**.
- 10 Type the **Refine** and **Filter** criteria.
- 11 Type the Title, Header, Footer, and Description.
- 12 Crosscheck the **Disk cost analysis** details.
- 13 Select **Add to Queue** checkbox, to process the report at a later point in time.
Update status via RSS field gets enabled.
- NOTE:** This option is not available if you have selected **Export Type** as **Quick View**.

- 14 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 15 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 16 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 17 Click the **Next** button.

EventTracker displays '**Review all the configuration details before submitting the Flex Reports request**' page.

- 18 Crosscheck the **Flex Reports parameters**, and then click the **Generate** button.

Note



You can select the **Add to queue** checkbox. EventTracker enables the **Show in** (Compliance Dashboard) and **Update status via RSS** dropdown list. Select an appropriate publishing option.

"**Enable publishing option**" will only be enabled if SMTP server is configured.

You can also exclude predefined columns from the report. EventTracker does not save this exclusion in the database.

Flex Reports - Trend - On Demand

Standard Column Flex Reports

- 1 In **EventTracker Enterprise**, move the mouse pointer over **Reports** menu, and then click **Flex Reports**.

OR

Click the **Reports** menu, and then click the **Flex reports** tab.

- 2 In the **Flex Reports** tree, expand **Logs**.
- 3 Right-click **Trend**, and then from the shortcut menu click **On Demand**.
(OR)

Click **Trend**, and then in the **Actions** pane click **On Demand**.

EventTracker displays the reports wizard.

- 4 Click **Next >>**.

EventTracker displays the '**Select required category/properties of events**' page.

- 5 Select the **Select an event category** option.

Click **Select categories** hyperlink, check the required category options in **Categories** dialog box, and then click the **OK** button.

(OR)

Select the **Select custom properties** option, and then select required event properties to analyze.

- 6 Click **Next >>**.

- 7 Select the **Groups/ Systems/ All Systems** from where the logs need to be monitored.

- 8 Click **Next >>**.

- 9 Select the report generation interval from the given options.

Field	Description
Select Interval	Select the number of days for which the report is to be generated. EventTracker considers events occurred during the selected number of days for analysis.
Select date range	Select the date range for which the report is to be generated.
Limit to time range	Set the time range for the selected interval or date range. EventTracker considers events occurred only in the given time range for analysis.

 **NOTE**

If **Limit to time range** option is selected with **Select date range** option, then only the time specified in **Limit to time range** will be considered for the report generation.

- 10 Select the **Export type** from the dropdown.

- 11 Select the **Sort by** option from the dropdown.

- 12 Click **Next >>**.

EventTracker displays '**You can narrow down the criteria by explicitly specifying the details**' page.

- 13 Select **Basic (Direct Query)** option:

Enter the **Refine** and **Filter** criteria.

Enter **Filter Event ID(s)** and **Event Source(s)** to be filtered out from the report.

You can type either Event ID(s) or Event Source(s) or both. All are optional values.

OR

Click **Advanced (Regular expression based query)** option, and then click the **Wizard** hyperlink to construct a query to **Match for specific information** or **Filter specific information**.

Please refer [Reg-Ex Help](#) section for more details.

- 14 Type the Title, Header, Footer, and Description, and then click the **Next >>**.

EventTracker displays '**Review cost details and configure the publishing options**' page.

- 15 Crosscheck the **Disk cost analysis** details.

- 16 Select **Add to queue (background processing)** checkbox, to process the report at a later point in time.

a/ **Update status via RSS** field gets enabled.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**

b/ Select the **Enable publishing option** checkbox to activate to deliver/notify the results via email

c/ Select appropriate publishing option from **Deliver results via E - mail** and **Notify results via E – mail**, and then enter the email ID(s) in **To E-mail** box.

d/ From the **Update status via RSS** field, select appropriate RSS Feed to get RSS notification.

 **NOTE**

It is not mandatory to select **Add to queue (background processing)** unless you wish to process the report at the later point of time.

- 17 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in **Compliance** dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 18 Click **Next >>**.

EventTracker displays '**Review all the configuration details before submitting the Flex Reports request**' page.

- 19 Crosscheck the **Reports parameters**.

- 20 Click the **Generate** button.

OR

If **Add to queue (background processing)** option is selected then click the Add to queue button.

Flex Reports - Summary - Queued

Standard Column Flex Reports

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.
Click **Reports** and move the mouse pointer to **Flex Report**
- 2 Click **Logs** in the flex report tree.
- 3 Click **On Demand** in the Actions pane, and then click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 4 Select category/custom properties, and click **Next >>**.
EventTracker displays the monitored Groups and Systems page.
- 5 Select the system(s) / group(s) / all systems), and then click **Next>>**.
- 6 Select the report generation Interval.
- 7 Select the **Format option** as **Summary**.
- 8 Select **Standard column** option.
- 9 Select the **Export type**.
NOTE: Selecting **Quick View** option disables 'Add to queue' checkbox.
- 10 Select Sort by option, and then click **Next>>**.
- 11 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 12 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 13 Crosscheck the **Disk cost analysis** details.
- 14 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 15 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 16 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 17 Click **Next>>**.
- 18 Crosscheck the **Reports parameters**.
- 19 Click **Add To Queue** button
(OR)
- 1 Log on to EventTracker Enterprise.
EventTracker displays the Home page.

- 2 Click **Flex Report**.
- 3 Click **Logs** in the Flex Report tree.
- 4 Click **Queued** in the Actions pane.
- 5 Click **New** in the Queued pane.
- 6 Click **Next >>**.
- 7 Select category/custom properties, and then click **Next >>**.
EventTracker displays the monitored Groups and Systems page.
- 8 Select the Groups / Systems / All Systemsall systems, and then click **Next>>**.
- 9 Select the report generation Interval.
- 10 Select the **Format option** as **Summary**.
- 11 Select the **Export type**, and then click **Next >>**.
NOTE: Selecting **Quick View** option disables 'Add to queue' checkbox.
- 12 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 13 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 14 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 15 Type the **Refine** and **Filter** criteria.
- 16 Type the Title, Header, Footer, and Description.
- 17 Crosscheck the **Disk cost analysis** details.
- 18 Crosscheck the **Reports parameters**.
- 19 Click **Add To Queue**.

Note



Quick View Export Type option is not available when you add a new Flex Reportsto queue by clicking Queued in the Actions pane.

"Enable publishing option" will only be enabled if SMTP server is configured.

Custom Column Flex Reports

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex Reports**.

- 3 Click **Logs** in the Flex Reports tree.
- 4 Click **On Demand** in the Actions pane.
- 5 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 6 Select the **Select category/custom properties** option.
- 7 Type appropriately in the relevant fields.
- 8 Click **Next >>**.
EventTracker displays the monitored Groups and Systems page.
- 9 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 10 Select the report generation Interval.
- 11 Select the **Format option** as **Summary**.
- 12 Select the **Custom column** option.

Export Type: Excel File (*.xls) is selected by default.

Note



If Export Type is selected as 'Excel file', then custom columns will be displayed as Row summary information and not as column in the report.

Selecting **Quick View** option disables 'Add to queue' checkbox.

EventTracker displays the 'Select or add Column(s) to display' page.

- 13 Click **Add New Column** button.
- 14 Enter the **Display name** and **Column name**.
- 15 Select **Add to select column** checkbox to add new columns to selected columns list.
- 16 Select **Save this column key** checkbox to save the new column names into the database.
- 17 Click the **Add** button.
EventTracker adds custom column.
- 18 In **Summary** and **Report Columns** field, click the up/down arrow keys to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.
- 19 Select the required report column, and then click up/down arrow to move the column. Select the **Sort by** option and then click **Next>>**.
- 20 Type the Refine and Filter criteria.

- 21 Type Title, Header, Footer, and Description.
 - 22 Crosscheck the Disk cost analysis details.
 - 23 Select the **Add to queue** checkbox.
 - 24 Enter Email ID in **To E-mail** box to deliver/notify the results via emails.
 - 25 Select RSS Feed from the **Update status via RSS** to get RSS notification.
 - 26 Crosscheck the Flex Reports parameters.
 - 27 Click **Add To Queue**.
-

Flex Reports - Detail - Queued

Standard Column Flex Reports

- 1 Log on to EventTracker Enterprise.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **flex reports**
- 3 Expand **Logs** in the Flex Reports tree.
- 4 Right-click **Detail**.
EventTracker displays the shortcut menu.
From the shortcut menu, choose **On Demand**.
(OR)
Select the **Summary** option and then click **On Demand** in the Actions pane.
EventTracker displays the Reports Wizard.
- 5 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 6 Select the **Select an event category** option.
Click **Select categories** hyperlink to select categories.
(OR)
Select the **Select custom properties** option.
Type appropriately in the relevant fields.
- 7 Click **Next >>**.
EventTracker displays the monitored Groups and Systems page.
- 8 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 9 Select the report generation Interval.
- 10 Select the **Format option** as **Detail**.

- 11 Select the **Export type**.
- 12 Select the **Sort by** option.
- 13 Type the **Refine** and **Filter** criteria.
- 14 Type the Title, Header, Footer, and Description.
- 15 Crosscheck the **Disk cost analysis** details.
- 16 Select the **Add to queue** checkbox, to process **the report** at a later point in time.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**
- 17 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 18 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 19 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**.
- 20 Crosscheck the Flex Reports parameters.
- 21 Click **Add To Queue**.

Note



"Enable publishing option" will only be enabled if SMTP server is configured.

Custom Column Flex Reports

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex Reports**
- 3 Expand Logs in the Flex Reports tree.
- 4 Right-click **Detail**.
EventTracker displays the shortcut menu.
From the shortcut menu, choose **On Demand**.
(OR)
Select the **Detail** option and then click **On Demand** in the Actions pane.
EventTracker displays the Reports Wizard.
- 5 Click **Next >>**.

EventTracker displays the 'Select required category/properties of events to analyze' page.

- 6 Select the **Select an event category** option.

Click **Select categories** hyperlink to select categories.

(OR)

Select the **Select custom properties** option.

Type appropriately in the relevant fields.

- 7 Click **Next >>**.

EventTracker displays the monitored Groups and Systems page.

- 8 Select the Groups / Systems / All Systems, and then click **Next>>**.

- 9 Select the report generation Interval.

- 10 Select the **Format option** as **Detail**.

- 11 Select the **Custom column** option, and then click **Next>>**.

EventTracker displays the 'Select or add Column(s) to display' page.

Export Type: Excel File (*.xls) is selected by default.

- 12 Click **Add New Column** button.

- 13 Enter the **Display name** and **Column** name.

- 14 Select **Add to select column** checkbox to add new columns to selected columns list.

- 15 Select **Save this column key** checkbox to save the new column names into the database.

- 16 Click the **Add** button.

EventTracker adds custom column.

- 17 In **Summary** and **Report Columns** field, click the up/down arrow keys to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.

Select the required report column, and then click up/down arrow to move the column.

EventTracker displays the selected columns in the **Summary** and **Report Columns** field.

- 18 Select the **Sort by** option and then click **Next>>**.

- 19 Type the **Refine** and **Filter** criteria.

- 20 Type Title, Header, Footer, and Description, and then click **Next>>**.

- 21 Crosscheck the **Disk cost analysis** details.

- 22 Select the **Add to queue** checkbox.

Update status via RSS field gets enabled.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**

- 23 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 24 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 25 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 26 Crosscheck the **Reports parameters**.
- 27 Click **Add To Queue**.

(OR)

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.
 - 2 Expand flex reports tree, and then select **Logs/ Detail**.
 - 3 Click **Queued** in the Actions pane.
 - 4 Click **New** in the Queued pane.
 - 5 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
 - 6 Select the **Select an event category** option.
Click **Select categories** hyperlink to select categories.
- (OR)**
- Select the **Select custom properties** option.
Type appropriately in the relevant fields.
- 7 Click **Next >>**.
EventTracker displays the monitored Groups and Systems page.
 - 8 Select the Groups / Systems / All Systems, and then click **Next>>**.
 - 9 Select the report generation Interval.
 - 10 Select the **Standard column** option, and then click **Next>>**.
 - 11 Select the **Format option** as **Detail**.
 - 12 Select the **Export type**.
 - 13 Select **Sort by** option, and then click **Next>>**.
 - 14 Type the **Refine** and **Filter** criteria, and then click **Next>>**.

- 15 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 16 Crosscheck the **Disk cost analysis** details.
- 17 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 18 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 19 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 20 Crosscheck the **Flex Reports parameters**.
- 21 Click **Add To Queue**.

Note



"**Enable publishing option**" will only be enabled if SMTP server is configured.

Export Type option '**Quick View**' is not available when you add a new Flex Reportsto queue by clicking Queued in the Actions pane.

Flex Reports - Trend - Queued

Standard Column Flex Reports

To generate Queued report

- 1 In **EventTracker Enterprise**, move the mouse pointer over **Reports** menu, and then click **Flex Reports**.

OR

Click the **Reports** menu, and then click the **Flex reports** tab.

- 2 In the **Flex Reports** tree, expand **Logs**.
- 3 Right-click **Trend**, and then from the shortcut menu click **Queued**.
(OR)

Click **Trend**, and then in the **Actions** pane click **Queued**.

EventTracker displays the reports wizard.

- 4 Click **Next >>**.
EventTracker displays the '**Select required category/properties of events**' page.
- 5 Select the **Select an event category** option.

Click **Select categories** hyperlink, check the required category options in **Categories** dialog box, and then click the **OK** button.

(OR)

Select the **Select custom properties** option, and then select required event properties to analyze.

- 6 Click **Next >>**.
- 7 Select the **Groups/ Systems/ All Systems** from where the logs need to be monitored.

Field	Description
File Transfer	Offline
Realtime	Online

- 8 Click **Next >>**.
- 9 Select the report generation interval from the given options.

Field	Description
Select Interval	Select the number of days for which the report is to be generated. EventTracker considers events occurred during the selected number of days for analysis.
Select date range	Select the date range for which the report is to be generated.
Limit to time range	Set the time range for the selected interval or date range. EventTracker considers events occurred only in the given time range for analysis.

NOTE

If **Limit to time range** option is selected with **Select date range** option, then only the time specified in **Limit to time range** will be considered for the report generation.

- 10 Select the **Export type** from the dropdown.
NOTE: Selecting **Quick View** option disables 'Add to queue' checkbox.
- 11 Select **Sort by** option from the dropdown.
- 12 Click **Next >>**.

EventTracker displays '**You can narrow down the criteria by explicitly specifying the details**' page.

13 Select **Basic (Direct Query)** option:

1. Enter the **Refine** and **Filter** criteria.
2. Enter **Filter Event ID(s)** and **Event Source(s)** to be filtered out from the report.

You can type either Event ID(s) or Event Source(s) or both. All are optional values.

OR

Click **Advanced (Regular expression based query)** option, and then click the **Wizard** hyperlink to construct a query to **Match for specific information** or **Filter specific information**.

Please refer [Reg-Ex Help](#) section for more details.

14 Type the Title, Header, Footer, and Description, and then click **Next >>**.

15 Crosscheck the **Disk cost analysis** details.

16 Select the **Add to queue (background processing)** checkbox to process the report at a later point in time.

Update status via RSS field gets enabled.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**

17 Select the **Enable publishing option** checkbox to activate to deliver/notify the results via email

18 Select appropriate publishing option from **Deliver results via E - mail** and **Notify results via E – mail**, and then enter the email ID(s) in **To E-mail** box.

19 From the **Update status via RSS** field, select appropriate RSS Feed to get RSS notification.

20 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in **Compliance** dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

21 Crosscheck the **reports parameters**, and then click the **Add to queue** button.

To generate queued report via On demand report option

You can add 'On demand' report as 'Queued' report if you select the Add to queue (background processing) checkbox while configuring the report.

- 1 In the **Flex Reports** tree, expand **Logs**.
 - 2 Right-click **Trend**, and then from the shortcut menu click **On Demand**.
- (OR)

Click **Trend**, and then in the **Actions** pane click **On Demand**.

EventTracker displays the reports wizard.

- 3 Click **Next >>**.

EventTracker displays the '**Select required category/properties of events**' page.

- 4 Select the **Select an event category** option.

Click **Select categories** hyperlink, check the required category options in **Categories** dialog box, and then click the **OK** button.

(OR)

Select the **Select custom properties** option, and then select required event properties to analyze.

- 5 Click **Next >>**.

- 6 Select the **Groups/ Systems/ All Systems** from where the logs need to be monitored.

- 7 Click **Next >>**.

- 8 Select the report generation Interval from the given options.

- 9 Select the **Format option** as **Trend**.

- 10 Select the **Export Type**.

- 11 Select **Sort by** option, and then click **Next >>**.

- 12 Type the **Refine** and **Filter** criteria, and then click **Next >>**.

- 13 Type the Title, Header, Footer, and Description, and then click **Next >>**.

- 14 Crosscheck the **Disk cost analysis** details.

- 15 Enter Email ID in **To E-mail** box to deliver/notify the results via emails.

- 16 Select RSS Feed from the **Update status via RSS** to get RSS notification.

- 17 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to be shown in Compliance Dashboard.

- 18 Crosscheck the **reports parameters**.

- 19 Click **Add To Queue**.

NOTE

Select the **Enable publishing option** checkbox and **Update status via RSS** drop-down list. Select an appropriate publishing option.

Quick View Export Type option is not available when you add new Flex Reports to queue by clicking Queued in the Actions pane.

Flex Reports - Summary - Scheduled

Standard Column Flex reports

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Logs** in the flex reports tree.
- 3 Click **Scheduled** in the Actions pane.
- 4 Click **New** in the Scheduled pane.
- 5 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 6 Select the **Select an event category/ Select custom properties** option, and then click **Next>>**.
- 7 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 8 Select the Schedule interval.

NOTE

If you select the Schedule Type as Daily / Weekly, then EventTracker displays the **Limit to time range** checkbox. Set the time range. EventTracker considers only events occurred in that specified time range.

- 9 Select the **Format option** as **Summary**.
 - 10 Select the **Export type**.
 - 11 Select the **Sort by** option, and then click **Next>>**.
 - 12 Type the Refine and Filter criteria, and then click **Next>>**.
 - 13 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 14 Crosscheck the **Disk cost analysis** details.
 - 15 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail. Type valid **To E-mail** address.
 - 16 Select RSS Feed from the **Update status via RSS** to receive RSS notification.
 - 17 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to be shown in Compliance Dashboard.
 - 18 Crosscheck the **reports parameters**.
 - 19 Click **Schedule**.
-

Custom Column flex reports

- 1 Click **Reports** dropdown and select **flex reports**
- 2 Click **Logs** in the Flex reports tree.
- 3 Click **Scheduled** in the Actions pane.
- 4 Click **New** in the Scheduled pane.
- 5 Click **Next >>**.

EventTracker displays the 'Select required category/properties of events to analyze' page.

- 6 Select the **Select event category / Select custom properties** option, and then click **Next>>**.
- 7 Select the Groups / Systems / All Systems , and then click **Next>>**.
- 8 Select the Schedule interval.

Note



If you select the Schedule Type as Daily / Weekly, then only EventTracker displays the **Limit to time range** checkbox. Set the time range. EventTracker considers only events occurred in that specified time range.

- 9 Select the **Format option** as **Summary**.
- 10 Select the **Custom Column** option, click the Next >> button.
Export Type: Excel File (*.xls) is selected by default.
- 11 Click **Add New Column** button.
- 12 Enter the **Display name** and **Column name**.
- 13 Select **Add to select column** checkbox to add new columns to selected columns list.
- 14 Select **Save this column key** checkbox to save the new column names into the database.
- 15 Click the **Add** button.
EventTracker adds custom column.
- 16 In **Summary** and **Report Columns** field, click the up/down arrow keys to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.
Select the required report column, and then click up/down arrow to move the column.
EventTracker displays the selected columns in the **Summary** and **Report Columns** field.

- 17 Select the **Sort by** option, and then click **Next>>**.
 - 18 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
 - 19 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 20 Crosscheck the **Disk cost analysis** details.
 - 21 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail. Type valid **To E-mail** address.
NOTE: "Enable publishing option" will only be enabled if SMTP server is configured.
 - 22 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
 - 23 Select RSS Feed from the **Update status via RSS** to receive RSS notification.
 - 24 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
 - 25 Crosscheck the **reports details**.
 - 26 Click **Schedule**.
-

Flex Reports - Detail - Scheduled

Standard Column Flex reports

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Logs** in the Flex reports tree, and then click **Scheduled** in the Actions pane.
- 3 Click **New** in the Scheduled pane.
- 4 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 5 Select the **Select an event category** option.
Click **Select categories** hyperlink to select categories.
(OR)
Select the **Select custom properties** option.
Type appropriately in the relevant fields.
- 6 Click **Next>>**.
- 7 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 8 Select the Schedule interval.

Note



If you select the Schedule Type as Daily Or Weekly, then only EventTracker displays the **Limit to time range** checkbox. Set the time range. EventTracker considers only events occurred in that specified time range.

- 9 Select the **Format option** as **Detail**.
- 10 Select the **Export type**.
- 11 Select **Sort by** option, and then click **Next>>**.
- 12 Type the Refine and Filter criteria.
- 13 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 14 Crosscheck the **Disk cost analysis** details.
- 15 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail. Type valid **To E-mail** address.
- 16 Select RSS Feed from the **Update status via RSS** to receive RSS notification.
- 17 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 18 Crosscheck the **Reports parameters**.
- 19 Click **Schedule**.

Note



"**Enable publishing option**" will only be enabled if SMTP server is configured.

Custom Column Flex reports

- 20 Click **Reports** dropdown and select **Flex reports**
- 21 Click **Logs** in the Flex reports tree.
- 22 Click **Scheduled** in the Actions pane.
- 23 Click **New** in the Scheduled pane.
- 24 Click **Next >>**.

EventTracker displays the 'Select required category/properties of events to analyze' page.

- 25 Select the **Select custom properties/ Select custom properties** option, and then click **Next>>**.

- 26 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 27 Select the Schedule interval.

Note



- 28 If you select the Schedule Type as Daily / Weekly, then only EventTracker displays the **Limit to time range** checkbox. Set the time range. EventTracker considers only events occurred in that specified time range. Select the **Format option** as **Detail**.
- 29 Select the **Custom column Flex Reports** option.
Export Type: Excel File (*.xls) is selected by default.
- 30 Click **Next>>**.
EventTracker displays the 'Select or add Column(s) to display' page.
- 31 Click **Add New Column** button.
- 32 Enter the **Display name** and **Column name**.
- 33 Select **Add to select column** checkbox to add new columns to selected columns list.
- 34 Select **Save this column key** checkbox to save the new column names into the database.
- 35 Click the **Add** button.
EventTracker adds custom column.
- 36 In **Summary** and **Report Columns** field, click the up/down arrow keys to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.

Select the required report column, and then click up/down arrow to move the column.

EventTracker displays the selected columns in the **Summary** and **Report Columns** field.
- 37 Select the **Sort by** option, and then click **Next>>**.
- 38 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 39 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 40 Crosscheck the **Disk cost analysis** details.
- 41 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail. Type valid **To E-mail** address.
- 42 Select RSS Feed from the **Update status via RSS** to receive RSS notification.
- 43 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to be shown in Compliance Dashboard.
- 44 Select **Sort by** option, and then click **Next>>**.
- 45 Crosscheck the **Flex reports parameters**.

46 Click **Schedule**.

Note



Quick View Export Type option is not available when you schedule an analysis.

EventTracker enables **Week Day** drop-down list only when you select the **Weekly** option from the **Schedule Type** drop-down list.

Flex reports - Trend - Scheduled

1 Click **Reports** dropdown and select **Flex reports**

2 Click **Logs** in the Flex reports tree.

3 Click **Scheduled** in the Actions pane.

4 Click **New** in the Scheduled pane.

5 Click **Next >>**.

EventTracker displays the 'Select required category/properties of events to analyze' page.

6 Click the **Select an event category / Select custom properties** option, and then click **Next>>**.

7 Select the systems / groups / all systems , and then click **Next>>**.

8 Select the Schedule interval.

Note



If you select the Schedule Type as Daily / Weekly, then only EventTracker displays the **Limit to time range** checkbox. Set the time range. EventTracker considers only events occurred in that specified time range.

9 Select the **Format option** as **Trend**.

10 Select the **Export type**.

11 Select **Sort by** option, and then click **Next>>**.

12 Type the **Refine** and **Filter** criteria, and then click **Next>>**.

13 Type the Title, Header, Footer, and Description, and then click **Next>>**.

14 Crosscheck the **Disk cost analysis** details.

- 15 Select the **Enable publishing option** checkbox to deliver or notify results via E-mail. Type valid **To E-mail** address.
NOTE: "Enable publishing option" will only be enabled if SMTP server is configured.
- 16 To deliver/notify the result via email, enter the email ID(s) in **To E-mail** box.
- 17 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 18 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 19 Crosscheck the **Reports** parameters.
- 20 Click **Schedule**.

Note



Quick View Export Type option is not available when you schedule a new analysis.

EventTracker enables **Week Day** drop-down list only when you select the **Weekly** option from the **Schedule Type** drop-down list.

Flex reports - Summary - Defined

Standard Column Flex reports

- 1 Log on to EventTracker Enterprise.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex reports**.
- 3 Click **Logs** in the Flex Reports tree.
- 4 Click **Defined** in the Actions pane.
- 5 Click **New**.
EventTracker displays the Reports Wizard.
- 6 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 7 Select the **Select an event category / Select custom properties** option, and then click **Next>>**.
EventTracker displays the monitored Groups and Systems page.
- 8 Select the Groups / Systems / All Systems , and then click **Next>>**.

EventTracker displays the 'Interval and More Options" page. Interval option is disabled for Defined Log Analyses.

- 9 Select the **Format option** as **Summary**.
 - 10 Select the **Export type**.
 - 11 Select the **Sort by** option, and then click **Next>>**.
 - 12 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
 - 13 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 14 Crosscheck the **flex reports parameters**.
 - 15 Click the **Save** button.
-

Custom Column Flex reports

- 1 Click **On Demand** in the Actions pane.
- 2 Click **Next >>**.
- 3 Select the **Select custom properties / Select custom properties** option, and then click **Next>>**.
- 4 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 5 Select the report generation Interval.
- 6 Select the **Format option** as **Summary**.
- 7 Select the **Custom column** option.

Export Type: Excel File (*.xls) is selected by default.

- 8 Click **Next>>**.

EventTracker displays the 'Select or add Column(s) to display" page.

- 9 Click **Add New Colum** button.
- 10 Enter the **Display name** and **Column name**.
- 11 Select **Add to select column** checkbox to add new columns to selected columns list.
- 12 Select **Save this column key** checkbox to save the new column names into the database.
- 13 Click the **Add** button.

EventTracker adds custom column.

- 14 In **Summary** and **Report Columns** field, click the up/down arrow keys to arrange the order of the columns that you wish to appear on the Summary and Detail sections of the report.

Select the required report column, and then click up/down arrow to move the column.

EventTracker displays the selected columns in the **Summary** and **Report Columns** field.

- 15 Select the **Sort by** option, and then click **Next>>**.
 - 16 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
 - 17 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 18 Select the **Add to queue** checkbox.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**
 - 19 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
 - 20 Select RSS Feed from the **Update status via RSS** to get RSS notification.
 - 21 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**.
 - 22 Click **Next>>**.
 - 23 Crosscheck the **Reports parameters**.
 - 24 Click **Save**.
-

Flex Reports - Detail - Defined

Standard Column Flex reports

- 1 Log on to EventTracker Enterprise.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex reports**
- 3 Click **Logs** in the Flex reports tree.
- 4 Click **Defined** in the Actions pane.
- 5 Click **New**.
EventTracker displays the Reports Wizard.
- 6 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze' page.
- 7 Select the **Select an event category / Select custom properties** option, and then click **Next>>**.
EventTracker displays the monitored Groups and Systems page.
- 8 Select the Groups / Systems / All Systems , and then click **Next>>**.

EventTracker displays the 'Interval and More Options" page. Interval option is disabled for Defined Log Analyses.

- 9 Select the **Format option** as **Detail**.
 - 10 Select the **Export type**.
 - 11 Select the **Sort by** option, and then click **Next>>**.
 - 12 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
 - 13 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 14 Crosscheck the **Reports parameters**.
 - 15 Click the **Save** button.
-

Flex reports - Trend - Defined

- 1 Log on to EventTracker Enterprise.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex reports**
Click **Logs** in the Flex reports tree.
- 3 Click **Defined** in the Actions pane.
- 4 Click **New**.
EventTracker displays the Reports Wizard.
- 5 Click **Next >>**.
EventTracker displays the 'Select required category/properties of events to analyze" page.
- 6 Select the **Select an event category / Select custom properties** option, and then click **Next>>**.
EventTracker displays the monitored Groups and Systems page.
- 7 Select the Groups / Systems / All Systems, and then click **Next>>**.
EventTracker displays the 'Interval and More Options" page. Interval option is disabled for Defined Log Analyses.
- 8 Select the **Format option** as **Trend**.
- 9 Select the **Export type**.
- 10 Select the **Sort by** option, and then click **Next>>**.
- 11 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 12 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 13 Crosscheck the **Reports parameters**.

- 14 Click the **Save** button.

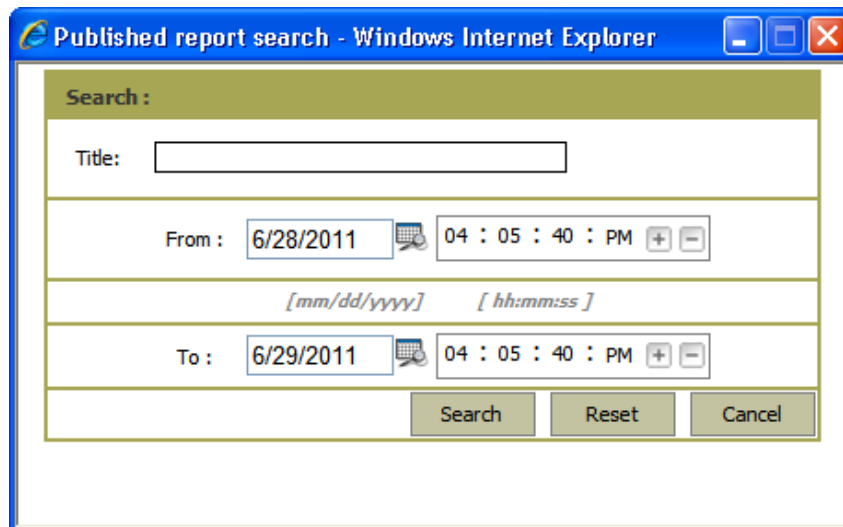
Searching generated Queued Flex Reports

To search generated Queued Flex Reports

- 1 Click  icon.

EventTracker displays the Search page.

Figure 219
Published Report
Search



By default, EventTracker searches reports that are generated in the past 24 hours. So, select the date appropriately from the Calendar control if you are not sure about the date.

- 2 Type appropriate details in the relevant fields.
 - 3 Click **Search**.
EventTracker displays the search result.
 - 4 Click **Show All** hyperlink to view all the generated reports.
-

Exporting Summary Report on Generated Flex Reports

To export summary report

- 1 Click  icon.

EventTracker displays the File Download pop up.

- 2 Click **Open** to view the report or **Save** to save the report in the hard disk.
-

Flex - Report Queue Statistics

To view Flex Report queue statistics

- Click the **Queued** link in the Actions pane.
EventTracker displays the statistics in the bottom pane.
-

Flex Reports Queue Statistics - Admin

To view Flex Reports queue statistics

- 1 Log in as user with Admin Privilege.
 - 2 Click the **Queued** in the Actions pane.
EventTracker displays the statistics in the bottom pane.
 - 3 Click **Show All User** Reports.
EventTracker displays the Log Flex ReportsReport Queue Statistics pane.
 - 4 Click **Show Reports Configured By Me** to view the reports configured by you.
-

Analyzing Alerts

EventTracker includes a category or group of event logs called *****Alerts*****. Those logs that require immediate attention are included in this group.

Alert Flex Reports shows event logs of this category.

Usage: Quickly review recent critical event logs.

Alert Flex reports - On Demand

- 1 Log on to **EventTracker Enterprise**.
EventTracker displays the Home page.
- 2 Click **Reports** dropdown and select **Flex reports**
EventTracker displays the Flex reports page.
- 3 Click **Alerts** in the Flex reports tree.
EventTracker displays the Alerts page.

- 4 Click **On Demand** in the Actions pane.
 - 5 Click **Next >>**.
 - 6 Select the Systems / Groups / all systems, and then click **Next>>**.
 - 7 Select the report generation **Interval**, **Format option** and **Export type**.
 - 8 Type the **Refine** and **Filter** criteria.
You can skip this step, if you do not have any criteria to set.
 - 9 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 10 Crosscheck the **Disk cost Analysis** details.
 - 11 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
 - 12 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
NOTE: This option is not available if you have selected **Export Type** as **Quick View**.
 - 13 Click **Next>>**.
 - 14 Click **Generate**.
-

Quick View

Quick View allows you to refine the result set. Quick View reports are not stored in the hard disk; you have to explicitly export those reports. Click the **Export** icon on the top strip to export the report. The exported reports can also be viewed in the Dashboard.

Note



You can select the **Add to queue** checkbox.

"**Enable publishing** option" will only be enabled if SMTP server is configured.

You can link a RSS Feed to the report.

Alert Flex reports - Queued

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Alerts** in the Flex reports tree.
- 3 Click **On Demand** in the Actions pane.
- 4 Click **Next >>**.
- 5 Select the Systems / Groups / all systems, and then click **Next>>**.

- 6 Select the report generation **Interval**, **Format option** and **Export type**, and then click **Next>>**.
- 7 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 8 Type the Title, Description, Footer, and Description, and then click **Next>>**.
- 9 Crosscheck **Disk Cost Analysis** details.
- 10 Select the **Add to queue** checkbox.

Update status via RSS field gets enabled.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**

- 11 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 12 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 14 Crosscheck the **Report parameters**.
- 15 Click **Add To Queue**.

(OR)

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Alerts** in the Flex reports tree.
- 3 Click **Queued** in the Actions pane.
- 4 Click **New** in the Queued pane.
- 5 Click **Next >>**.
- 6 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 7 Select the report generation **Interval**, **Format option** and **Export type**, and then click **Next>>**.
- 8 Type the Refine and Filter criteria, and then click **Next>>**.
- 9 Type the Title, Description, Footer, and Description, and then click **Next>>**.
- 10 Crosscheck the **Disk Cost Analysis** details.
- 11 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 12 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 14 Click **Next>>**.

- 15 Crosscheck the Flex reports Parameters.
- 16 Click **Add To Queue**.

Note



Quick View Export Type option is not available when you add a new Flex Report to queue.

Alert Flex reports - Scheduled

- 1 Click **Reports** dropdown and select **Flex reports**.
- 2 Click **Alerts** in the Flex reports tree.
- 3 Click **Scheduled** in the Actions pane.
- 4 Click **New** in the Scheduled pane.
- 5 Click **Next >>**.
- 6 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 7 Select the **Schedule interval**, **Format option** and **Export Type**, and then click **Next>>**.
- 8 Type the Refine and Filter criteria, and then click **Next>>**.
- 9 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 10 Crosscheck **Disk Cost Analysis** details.
- 11 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 12 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

NOTE: This option is not available if you have selected **Export Type** as **Quick View**.

- 14 Click **Next>>**.
- 15 Crosscheck the Flex reports **parameter** details.
- 16 Select the **Enable publishing option** checkbox.

NOTE: "Enable publishing option" will only be enabled if SMTP server is configured.

- 17 Click **Schedule**.

Note



Quick View Export Type option is not available when you schedule an analysis.

EventTracker enables **Week Day** drop-down list only when you select the **Weekly** option from the **Schedule Type** drop-down list.

Analyzing Log Volume

Filter and display event logs based on user defined criteria. The user can define the filter (or exclude) string as well as specify the output format.

Usage: Forensic Flex Report of specific events, broad searches per criteria with subsequent sorting and ordering of the result set.

Flex Reports Logs - On Demand

Event Categories

- 1 Log on to **EventTracker Enterprise**.
- 2 Click **Reports** dropdown and select **Flex reports**
- 3 Click **Log Volume** in the Flex Report tree.
- 4 Click **On Demand** in the Actions pane.
- 5 Click **Next >>**.
- 6 Click the **Select an Event Category** option.
- 7 Select a category from **Category** drop-down list, and then click **Next>>**.
- 8 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 9 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
- 10 Type the Refine and Filter criteria, and then click **Next>>**.
- 11 Type the Title, Header Footer, and Description, and then click **Next>>**.
- 12 Crosscheck the **Disk cost Analysis** details.
- 13 Select the **Add to queue** checkbox.
Update status via RSS field gets enabled.
NOTE: You can skip this step if you wish to generate the report immediately.
- 14 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 15 Select RSS Feed from the **Update status via RSS** to get RSS notification.

- 16 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 17 Click **Next>>**.
- 18 Crosscheck the **Flex reports parameters**.
- 19 Crosscheck the Flex reports details.
- 20 Click **Generate**.

Custom properties

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Log Volume** in the Flex Report tree.
- 3 Click **On Demand** in the Actions pane.
- 4 Click **Next >>**.
- 5 Select the **Select Custom Properties** option.
- 6 Enter appropriately in the relevant fields.
- 7 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 8 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
- 9 Type the Refine and Filter criteria, and then click **Next>>**.
- 10 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 11 Crosscheck the **Disk cost Analysis** details.
- 12 Select / enter appropriately in the relevant fields.
- 13 Select the **Add to queue** checkbox.
Update status via RSS field gets enabled.
NOTE: You can skip this step if you wish to generate the report immediately.
- 14 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 15 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 16 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 17 Click **Next>>**.
- 18 Crosscheck the **Flex reports parameters**.
- 19 Click **Add to Queue** button.

Note

"Enable **publishing** option" will only be enabled if SMTP server is configured.

Event Id

- 1 Click **Reports** dropdown and select **Flex reports**
 - 2 Click **Log Volume** in the Flex Report tree.
 - 3 Click **On Demand** in the Actions pane.
 - 4 Click **Next >>**.
 - 5 Select the **Select by Event Id** option.
 - 6 Select **Display all records** or **Display only top "n" records** option.
 - 7 Select the Groups / Systems / All Systems, and then click **Next>>**.
 - 8 Select the report generation **Interval** and **Export type**.
 - 9 Type the Refine and Filter criteria, and then click **Next>>**.
 - 10 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 11 Crosscheck the **Disk cost Analysis** details.
 - 12 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
 - 13 Select RSS Feed from the **Update status via RSS** to get RSS notification.
 - 14 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
 - 15 Click **Next>>**.
 - 16 Crosscheck the **Reports parameters**.
 - 17 Click **Generate/ Add to queue**.
-

Flex reports Logs- Queued

- 1 Click **Reports** dropdown and select **Flex reports**.
- 2 Click **Log Volume** in the Flex reports tree.
- 3 Click **On Demand** in the Actions pane.
- 4 Click **Next >>**.
- 5 Select the **Event categories/Custom properties/Event Id** option.
- 6 Select/enter appropriately in the relevant fields, and then click **Next >>**.
- 7 Select the Groups / Systems / All Systems, and then click **Next >>**.
- 8 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
- 9 Type the Refine and Filter criteria, and then click **Next >>**.
- 10 Type the Title, Header, Footer, and Description, and then click **Next >>**.
- 11 Crosscheck **Disk cost analysis** details.
- 12 Select the **Add to queue** checkbox.
Update status via RSS field gets enabled.

- 13 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 14 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 15 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 16 Click **Next>>**.
- 17 Crosscheck the **Reports parameters**.
- 18 Click **Add To Queue**.
- (OR)
- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Log Volume** in the Flex Report tree.
- 3 Click **Queued** in the Actions pane.
- 4 Click **New** in the Queued pane.
- 5 Click **Next >>**.
- 6 Select the **Event categories/Custom properties/Event Id** option.
- 7 Select/enter appropriately, and then click **Next>>**.
- 8 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 9 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
- 10 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 11 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 12 Crosscheck the **Disk cost Analysis** details.
- 13 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 14 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 15 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 16 Click **Next>>**.
- 17 Crosscheck the **Reports parameters**.
- 18 Click **Add To Queue**.

Note



"Enable **publishing** option" will only be enabled if SMTP server is configured.

Quick View Export Type option is not available when you schedule a new analysis.

Flex reports Logs- Scheduled

- 1 Click **Reports** dropdown and select **Flex reports**.
- 2 Click **Log Volume** in the Flex reports tree.
- 3 Click **Scheduled** in the Actions pane.
- 4 Click **New** in the Scheduled pane.
- 5 Click **Next >>**.
- 6 Select the **Event categories/Custom properties/Event Id** option.
- 7 Select/enter appropriately in the relevant fields,, and then click **Next>>**.
- 8 Select the Groups / Systems / All Systems , and then click **Next>>**.
- 9 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
- 10 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 11 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 12 Crosscheck the **Disk cost Analysis** details.
- 13 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 14 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 15 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 16 Click **Next>>**.
- 17 Crosscheck the **Reports parameters**.
- 18 Click **Schedule**.

Note



"Enable **publishing** option" will only be enabled if SMTP server is configured.

Quick View Export Type option is not available when you schedule a new analysis.

EventTracker enables **Week Day** drop-down list only when you select **Weekly** as **Schedule Type**.

Analyzing Suspicious Traffic

The classic virus infection causes unrecognized EXEs to begin accessing the network.

When enabled, the EventTracker Agent for Windows can be configured with a white-list of known ports or application and report exceptions. This helps to identify potentially suspicious traffic. The report uses a database of known infections per port to identify potential threats.

Usage: After suitably configuring the EventTracker Agent for Windows, this report is used to report on unusual traffic from unrecognized EXEs.

- Select Suspicious Traffic Only (SNAM) option in Agent Configuration window under Network Connection Monitor tab prior to generating Suspicious Traffic Flex Report reports.
- To receive alerts on the occurrence of suspicious traffic, select Suspicious Network Activity Alerts option in the Manager Configuration window.

Flex reports Suspicious Traffic - On Demand

- 1 Click **Reports** dropdown and select **Flex reports**.
- 2 Click **Suspicious Traffic** in the Flex reports tree.
- 3 Click **On Demand** in the Actions pane.
- 4 Click **Next >>**.
- 5 Select the Groups / Systems / All Systems, and then click **Next >>**.
- 6 Select the report generation **Interval** and **Export type**, and then click **Next >>**.
- 7 Type the **Refine** and **Filter** criteria, and then click **Next >>**.
- 8 Type the Title, Header, Footer, and Description, and then click **Next >>**.
- 9 Crosscheck the **Disk cost Analysis** details.
- 10 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 11 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 12 Click **Next >>**.
- 13 Crosscheck the Flex reports parameters.
- 14 Click **Generate**.

Note



You can also select the **Add to queue** checkbox. EventTracker enables **Update status via RSS** field gets enabled.

"Enable publishing option" will only be enabled if SMTP server is configured.

Flex Reports Suspicious Traffic - Queued

- 1 Click **Reports** dropdown and select **Flex reports**..
 - 2 Click **Suspicious Traffic** in the Flex reports tree.
 - 3 Click **On Demand** in the Actions pane.
 - 4 Click **Next >>**.
 - 5 Select the Groups / Systems / All Systems, and then click **Next>>**.
 - 6 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
 - 7 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
 - 8 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 9 Crosscheck **Disk cost Analysis** details.
 - 10 Select the **Add to queue** checkbox.
 - 11 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
 - 12 Select RSS Feed from the **Update status via RSS** to get RSS notification.
 - 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
 - 14 Click **Next>>**.
 - 15 Click **Add To Queue**.
- (OR)
- 1 Click **Reports** dropdown and select **Flex reports**.
 - 2 Click **Suspicious Traffic** in the Flex reports type.
 - 3 Click **Queued** in the Actions pane.
 - 4 Click **New** in the Queued pane.
 - 5 Click **Next >>**.
 - 6 Select the Groups / Systems / All Systems , and then click **Next>>**.
 - 7 Select the report generation Interval and Export type, and then click **Next>>**.
 - 8 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
 - 9 Type the Title, Header, Footer, and Description, and then click **Next>>**.
 - 10 Crosscheck the **Disk cost Analysis** details.
 - 11 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.

- 12 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 14 Crosscheck the **Reports parameter**.
- 15 Click **Add To Queue**.

Note



"Enable **publishing** option" will only be enabled if SMTP server is configured.

Quick View Export Type option is not available when add new Flex Report to queue by clicking Queued in the Actions pane.

Flex Reports Suspicious Traffic - Scheduled

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Suspicious Traffic** in the Flex reports tree.
- 3 Click **Scheduled** in the Actions pane.
- 4 Click **New** in the Scheduled pane.
- 5 Click **Next >>**.
- 6 Select the Groups / Systems / All Systems, and then click **Next>>**.
- 7 Select the report generation **Interval** and **Export type**, and then click **Next>>**.
- 8 Type the **Refine** and **Filter** criteria, and then click **Next>>**.
- 9 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 10 Crosscheck the **Disk cost Analysis** details.
- 11 Select / enter appropriately in the relevant fields.
- 12 Click **Next >>**.
- 13 Crosscheck the Flex reports parameters.
- 14 Click **Schedule**.

Note

Type valid **To E-mail** address to deliver or notify results via E-mail. Select RSS Feed from the **Update status via RSS** to get RSS notification.

"Enable **publishing** option" will only be enabled if SMTP server is configured.

Quick View Export Type option is not available when you schedule an analysis.

EventTracker enables **Week Day** drop-down list only when you select the **Weekly** as **Schedule Type**.

Analyzing ROI

EventTracker collects statistics of logs received, alerts issued, reports generated, system and service downtime etc. User defined variables such as time saved by process automation and labor hour cost information is used to compute cost and time savings accrued.

Person Hour

Time (in seconds) taken for manual Flex Report - The time required to perform each function manually. When automated by EventTracker, this is the time saved. These values are used to compute overall time/cost savings.

Labor rates (per hour) - Shows the fully loaded labor cost per hour of a system administrator's time. These values are used to compute total cost savings.

This option helps you generate On Demand reports in the foreground. You can also Queue or Schedule Person Hour Analysis.

On Demand

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Cost Savings** in the Flex Report tree.
- 3 Click **On Demand** in the Actions pane.
- 4 Click **Next >>**.
- 5 Select the **Interval**, **Format option**, **Export type**, and **Chart type**.
- 6 Type the Title, Header, Footer, and Description.
- 7 Crosscheck the **Disk cost Analysis** details.
- 8 Select the **Add to queue** checkbox.
Update status via RSS field gets enabled.
NOTE: You can skip this step if you wish to generate the report immediately.
- 9 To deliver/notify the result via email, enter the email ID's in **To E-mail** box.
- 10 Select RSS Feed from the **Update status via RSS** to get RSS notification.
- 11 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.

- 12 Click **Next>>**.
- 13 Crosscheck the Flex Report details.
- 14 Click **Generate/ Add to queue**.

Queued

- 1 Click **Reports** dropdown and select **Flex reports**
- 2 Click **Cost Savings** in the Flex Report tree.
- 3 Click **Queued** in the Actions pane.
- 4 Click **New** in the Queued pane.
- 5 Click **Next >>**.
- 6 Select the **Interval**, **Format option**, **Export type**, and **Chart type**.
- 7 Type the Title, Header, Footer, and Description.
- 8 Select the **Enable publishing option** checkbox.
- 9 Select the **Deliver results via E-mail** option to deliver the report to the specified receiver mail id(s).
- 10 Select the **Notify results via E-mail** option to notify the report generation alone to the specified receiver mail id(s).
- 11 To deliver/notify the result as a attachment via email, enter the email ID's in **To E-mail** box.
- 12 Select a RSS feed from the **Update status via RSS** drop-down list to receive RSS Alert notification.
- 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 14 Crosscheck the **Flex reports parameters**.
- 15 Click **Add to queue**.

Scheduled

- 1 Click **Reports** dropdown and select **Flex reports**.
- 2 Click **Cost Savings** in the Flex Report tree.
- 3 Click **Scheduled** in the Actions pane.
- 4 Click **New** in the Scheduled pane.
- 5 Click **Next >>**.
- 6 Select the **Schedule type** and **Schedule time**.
- 7 Select the Format option, Export type, and Chart type, and then click **Next>>**.
- 8 Type the Title, Header, Footer, and Description, and then click **Next>>**.
- 9 Select the **Enable publishing option** checkbox.

Select the **Deliver results via E-mail** option to deliver the report to the specified receiver mail id(s).

- 10 Select the **Notify results via E-mail** option to notify the report generation alone to the specified receiver mail id(s).
- 11 To deliver/notify the result as a attachment via email, enter the email ID's in **To E-mail** box.
- 12 Select a RSS feed from the **Update status via RSS** drop-down list to receive RSS Alert notification.
- 13 In **Show in** dropdown, select the **Compliance Dashboard** option, if you want the results to appear in Compliance Dashboard.
- 14 Click **Next>>**.
- 15 Crosscheck the **Reports parameters**.
- 16 Click **Schedule**.

Note



Quick View Export Type option is not available when you schedule/queue an analysis.

EventTracker enables **Week Day** drop-down list only when you select the **Weekly** as **Schedule Type**.

"Enable publishing option" will only be enabled if SMTP server is configured.

Chapter 14

Configuring RSS Feeds

In this chapter, you will learn how to:

- [Configure & manage RSS Feeds](#)

RSS Feeds

RSS/XML feeds can send notification to your computer upon generation of advanced reports or alerts raised by EventTracker. Contents will fly to your desktop faster than an e-mail notification.

EventTracker does not delete a RSS Feed permanently, when you delete it, rather it does make it inactive.

Adding RSS Feeds

This option helps you add RSS feeds.

To add RSS feeds

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** dropdown, and then click **RSS**.

EventTracker displays the **RSS Feeds** page.

Figure 220
RSS Feeds



Table 81

Field	Description
Feed Name	Name of the feed.
Description	Short description of the feed.
Added By	Name of the user who configured the feed.
Added Date	Date and time when the feed was added.
Show	Select an option to view by status of the feeds.

Table 82

Click	To
Add New	Add new feeds.
Edit	

Click	To
Delete	Delete feeds. Once the feeds are deleted, they are not deleted from the db permanently; rather EventTracker changes the status of the feeds as Inactive . Inactive feeds cannot be reactivated.

3 Click **Add New**.

EventTracker displays the RSS Feeds dialog box.

Figure 221
RSS Feeds

4 Provide a **Feed Name**, and relevant description in **Feed Description** for future reference.

5 Click **Save**.

EventTracker displays the **RSS Feeds** page with newly added RSS feed.

Figure 222
RSS Feeds

Feed Name	Description	Added By	Added Date	Active
EventTracker - Alerts Feed	feed configured to be updated when an alert is generated.	Sonal	7/16/2012 10:40:45 PM	<input checked="" type="checkbox"/>
EventTracker - Security Feed	Feed configured to be updated when security related events occur.	Sonal	7/16/2012 10:41:40 PM	<input type="checkbox"/>

NOTE

You need to have IE v7.0 and above to subscribe to RSS Feeds. You can also add the feed links to RSS Reader.

Delete RSS Feeds

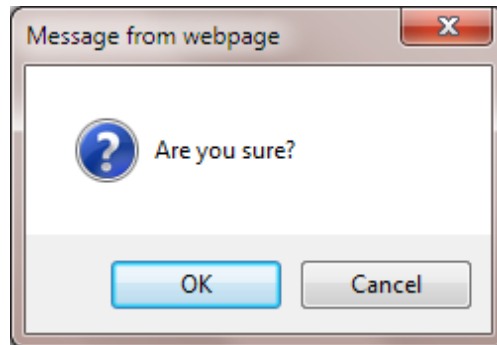
This option helps you delete RSS feeds.

To delete RSS feeds

- 1 Select the feed that you wish to delete.
- 2 Click **Delete**.

EventTracker displays the confirmation message box.

Figure 223
EventTracker
Console – message
box



- 3 Click **OK**.
- EventTracker deletes the selected RSS feed from the list.
-

Chapter 15

Managing System Groups

In this chapter, you will learn how to:

- [Auto Discover System Groups](#)
- [Add Logical System Groups](#)
- [View System Status](#)
- [Start Agent Service](#)
- [View System Details](#)
- [Manage Asset Value](#)

About Systems Manager

This is a centralized location to discover and manage the systems that are present in an enterprise domain and to deploy the remote agents.

Systems manager helps you to:

- Automatically discover enterprise domains and systems
- Manually add systems if you opt to
- Manage EventTracker Windows agent and Change Audit agent
- Manage logical system groups

To start System manager

- 1 Click the **Admin** dropdown, and then select **Systems**.

EventTracker displays **Systems** manager screen.

Figure 224
System Manager

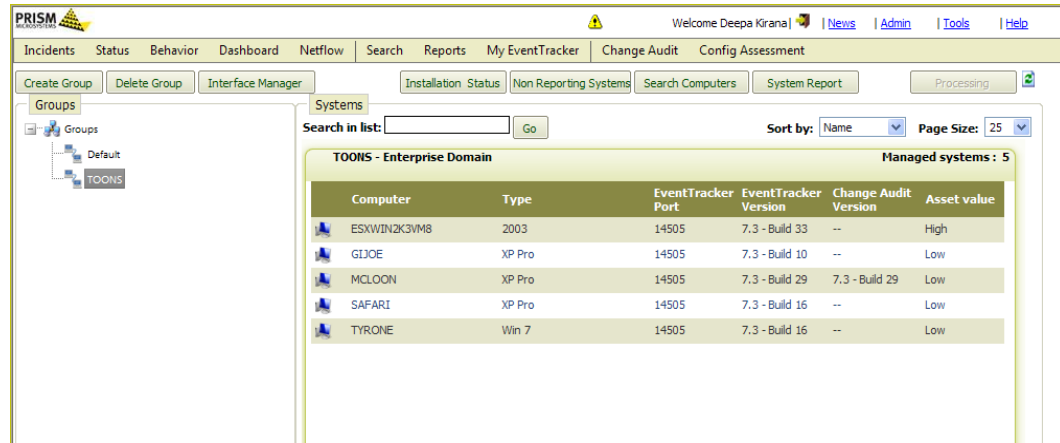


Table 83

Field	Description
Computer	Name of the computer or name of the DLA / NetFlow instance.
Type	Operating system installed on the computer.
EventTracker Port	Port through which the EventTracker Windows agent and the EventTracker manager communicates.
EventTracker Version	Displays EventTracker version and build number.
Change Audit Version	Displays Change Audit version and build number.
Asset Value	Asset value indicates how important or critical the computer is.

Table 84

Click	To
-------	----

Click	To
Create Group	Create logical system groups.
Delete Group	Delete logical system groups.
Interface Manager	Modify Netflow interface details.
Installation Status	Checks install / upgrade / uninstall status of EventTracker Windows agent / Change Audit agent. Also, to check status of computer search.
Non Reporting Systems	Search a list of systems which have not reported any events to the EventTracker manager in a specific duration of time.
Search Computers	Manually add enterprise domains and computers.
System Report	Generate status report of managed and unmanaged computers.
Auto Discover	Automatically discover enterprise domains and computers.

Discover Modes

System Manager adds domains and computers in two modes, namely **Auto** and **Manual**. In auto-discover modes 'System' manager creates system groups based on enterprise domains.

Auto Discover mode is easy to use and is recommended for networks having less than 100 systems.

Auto Discover Mode

The **Auto Discovery** mode detects and adds all systems found on all trusted domains. The auto discovery process includes an initial quick detection for systems and a background search for more systems.

To automatically discover systems

- 1 Click the **Admin** dropdown, and then click **Systems**.
 - 2 Click **Auto Discover** at the upper-right corner.
System manager displays confirmation message.
 - 3 Click the **Ok** button.
System manager automatically starts adding domains and computers.
- OR
- Click **Cancel** to cancel auto-discovery.

 NOTE

Only the user who initiated auto-discovery can cancel.

Manual Mode

Unlike in 'Auto discover' mode, system manager will not discover any domains or computers in this mode. You have to add them manually.

Manually Adding Computers

In 'Auto discover' mode, the 'System' manager automatically discovers domains and computers when you keep adding them in your enterprise. All you need to do is to refresh the System manager. However, in 'Manual' mode, you have to add them explicitly.

Adding a Single Computer

This option enables you to add a computer.

To add a single computer

- 1 Click the **Admin** dropdown, and then click **Systems**.
EventTracker displays **Systems** manager page.
- 2 Click **Search Computers** button.
System Manager displays the **Add Computer(s)** pop-up window.

Figure 225
Add Computer(s) –
Add a single
computer

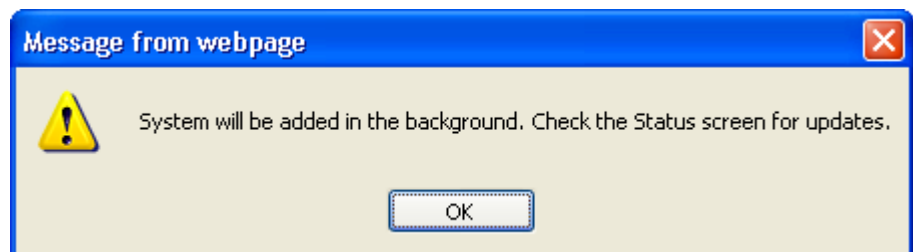
Table 85


Field	Description
Add a single computer (by name or by IP address)	Select this option to add a single computer.
Add a group of computers from available domains	Select this option to add a group of computers.
Add computers belonging to an IP range	Select this option to add computers from an IP subnet.

- 3 Select the **Add a single computer (by name or by IP address)** option, if not selected.
- 4 Type the name of the computer in the **Enter computer name or IP Address** field.
- 5 Provide valid **User Credentials**.
- 6 Click **Ok**.

System manager displays the message box.

Figure 226
Add Computers –
message box



- 7 Click **OK**.
- 8 Click the  icon to refresh the **Systems** manager.

- 9 Click **Installation Status** button to view the status.
- 10 Edit a system group and add the newly added Computer to that group.

Adding a Group of Computers

This option enables you to add a group of Computers. Note that it is possible to add Computers only with available Domains.

To add a group of computers

- 1 Select the **Add a group of Computers from available Domains** option.

Figure 227
Add Computer(s)
window – Add a
group of computers

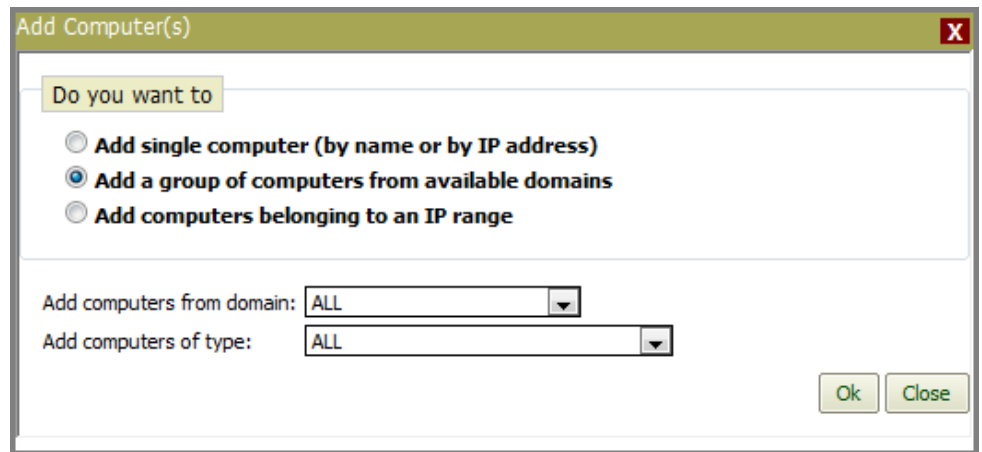
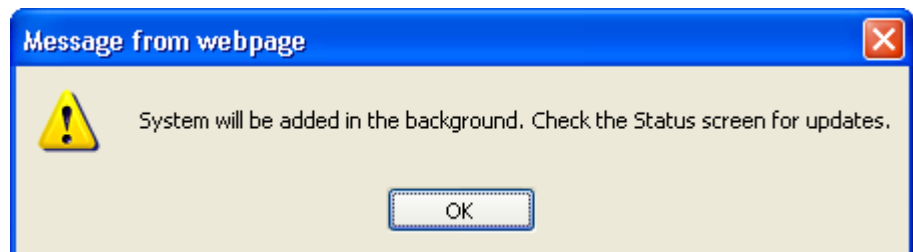



Table 86

Field	Description
Add computers from domain	This drop-down list lists the available domains. Select a domain from where you want to add computers.
Add computers of type	Select a system type from the drop-down list.

- 2 Select appropriate options.
- 3 Click **OK**.

Figure 228
Add a group of
computers –
message box



- 4 Click **OK**.
- 5 Click the  icon to refresh the **Systems** manager.

Adding a Group of Computers from an IP subnet

This option enables you to create a new logical Group of systems based on IP subnet, especially to add legacy Workgroup computers.


To add computers from an IP subnet

- 1 Select the **Add computers belonging to an IP range** option.

Figure 229 Add Computer(s) – Add computers from an IP subnet

Table 87

Field	Description
IP range	Type the IP address range to be added.
DNS discovery alone	The specified IP range will be discovered using DNS method.
SNMP discovery alone	The specified IP range will be discovered using SNMP method.
Ping discover alone	The specified IP range will be discovered using Ping method.
All	The specified IP range will be discovered using DNS /SNMP/Ping method.
SNMP community string	A password which is necessary to read/write SNMP data.

- 2 Type appropriately in the relevant fields.
- 3 Click **OK**.
- 4 Click the  icon to refresh the **Systems** manager.
The computers are added to the selected domain.

Logical System Groups

Logical system groups help you group computers that you wish to monitor exclusively. You can select computers by O/S type, from IP subnet or pick them manually.

Creating a New Logical Group – System Type

This option enables you to create a new logical Group of systems based on system type.

To create a new logical group and add systems based on System Type

- 1 Open the **Systems** manager.
- 2 Click **Create Group** button.

System manager displays the **Create Group** dialog box window

Figure 230
Create Group –
System Type

Table 88

Field	Description
Group Name	Type the group name in this field. The group name should be unique.
Group Description	Type the group description in this field.
Group Type	Select the group type option. The options are System Type, IP Subnet and Select Manually. System Type – Enables you to add the selected system type to the group. IP Subnet – Enables you to add the IP subnet to the group.

Field	Description
	Select Manually – Enables you to add the systems manually from the available list to the group.

- 3 Type appropriately in the relevant fields.

Figure 231
Create Group –
System Type

- 4 Click **Next**.

If you select the System Type option, System Manager displays the Create Group dialog box with the option to select O/S type.

Figure 232
Create Group –
System Type

- 5 Select the system type from the Select System Type drop-down list.
- 6 Click **Finish**.

System Manager creates and populates the newly created system group with the systems that have O/S type selected.

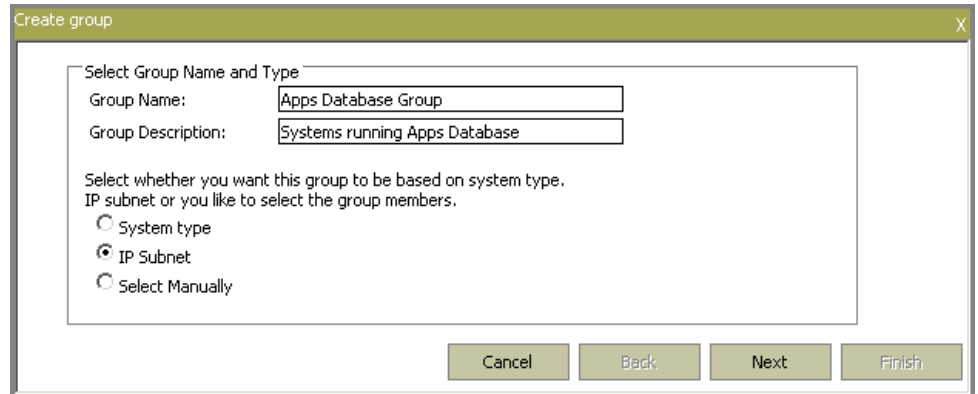
Creating a New Logical Group – IP Subnet

This option enables you to create a new logical Group of systems based on IP subnet.

To create a new logical group and add systems based on IP subnet

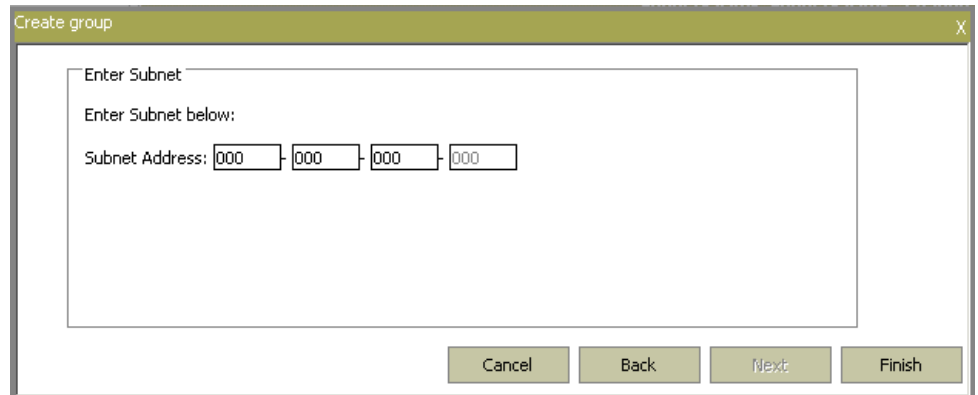
- 1 Select the **IP Subnet** option in the Create Group pop-up window.

Figure 233
Create Group – IP
Subnet



- 2 Click **Next**.
System Manager displays the Enter subnet pane.

Figure 234
Create Group – IP
Subnet



- 3 Type the **Subnet Address**.
- 4 Click **Finish**.

System Manager creates and populates the newly created system group with the systems from the IP subnet selected.

Creating a New Logical Group – Manual Selection

This option enables you to create a new logical Group of systems and manually add Computers to that Group.

To create a new logical group and add systems manually to that group

- 1 Select the **Select Manually** option in the Create Group pop-up window.

Figure 235
Create Group –
Select Systems
Manually

The 'Create group' dialog box has a title bar with 'Create group' and a close button 'X'. The main area is titled 'Select Group Name and Type'. It contains two text input fields: 'Group Name:' with the value 'Apps Database Group' and 'Group Description:' with the value 'Systems running Apps Database'. Below these fields is a text label: 'Select whether you want this group to be based on system type, IP subnet or you like to select the group members.' There are three radio button options: 'System type', 'IP Subnet', and 'Select Manually', which is selected. At the bottom right are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'.

- 2 Click **Next**.

System Manager displays the Create Group pop-up window with the option to select managed and unmanaged systems.

Figure 236
Create Group –
Select Systems
Manually

The 'Create group' dialog box is now in the 'Select Systems' step. It has a title bar with 'Create group' and a close button 'X'. The main area is titled 'Select Systems' and contains the text 'Select systems that you want to add'. There is a checkbox labeled 'Show Managed Systems only' which is currently unchecked. Below the checkbox is a list box containing the following system names: ESXWEBDOC, ALICE-II, BALOO, BALOO-II, CHARLIE, DEXTER, and DONALD II. At the bottom right are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'.

- 3 Select the **Show managed systems only** checkbox to view only managed systems in the list.
- 4 Select the systems you want to add to the group from the list.
- 5 Click **Finish**.

System Manager creates and populates the newly created system group with the systems selected.

Modifying a Group

Though the System Manager groups the auto discovered computers under their respective groups, you can move systems back and forth between groups as you deem fit.

To modify a Group

- 1 Open the System Manager.
- 2 Right-click the group that you want to edit.
System Manager displays the shortcut menu.
- 3 From the shortcut menu, choose **Edit**.
System Manager displays the details of the group with the available systems list.

Figure 237
Edit Group

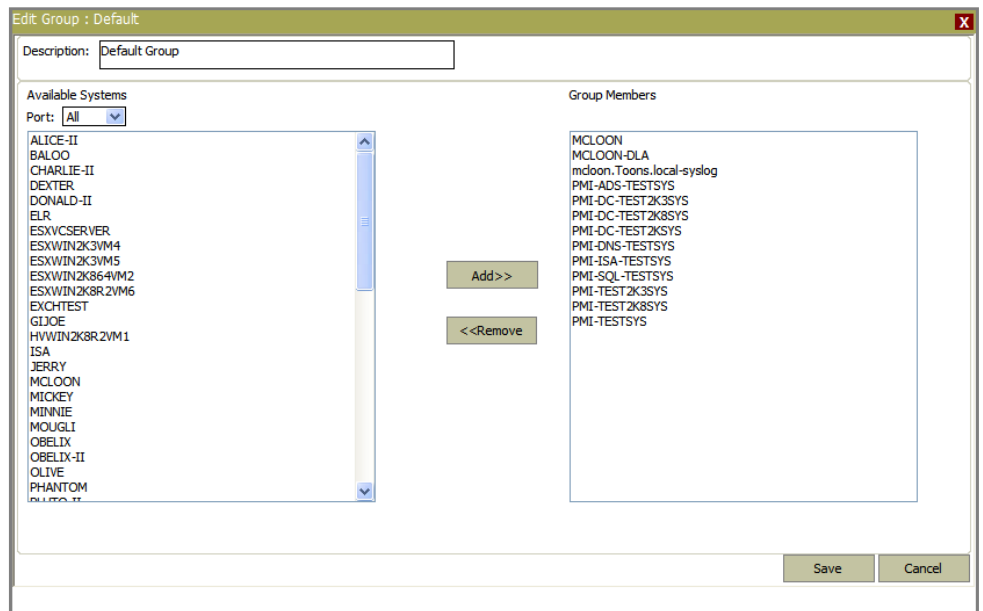


Table 89

Field	Description
Description	Type the system-related information in this field.
Group Members	Select the computer that you want to remove from the group. Click <<Remove.
Available Systems	Select the computer that you want to add to the group. Click Add >>. The selected computer is added to the list of Group Members.
Port	Select the port number from the dropdown list.

- 4 Edit appropriately and then click **Save**.

Deleting a Group

This option enables you to delete an existing Group.

To delete a Group

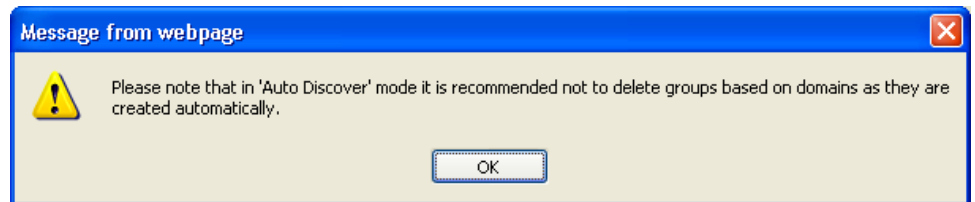
- 1 Open the System Manager.
- 2 Select the group and then click **Delete Group**.

(OR)

Click **Delete Group**.

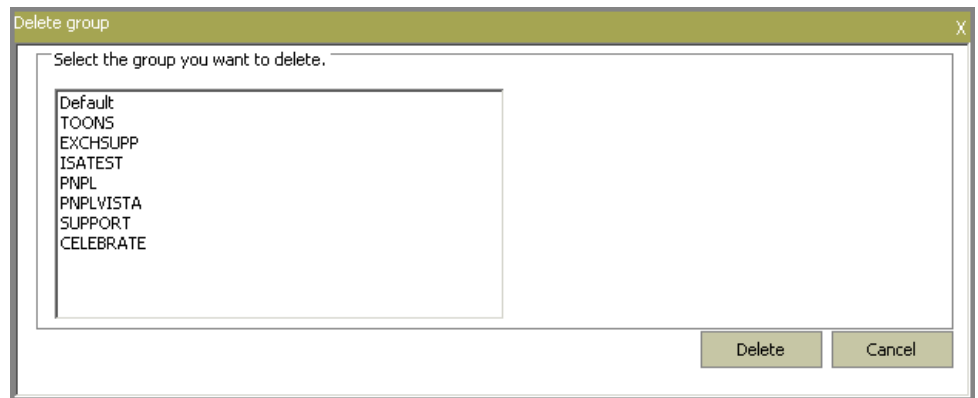
System Manager displays the confirmation message box.

Figure 238
Delete Group



- 3 Click **OK**.
System Manager displays the list of system groups

Figure 239
Delete Group



- 4 Select a group and then click **Delete**.

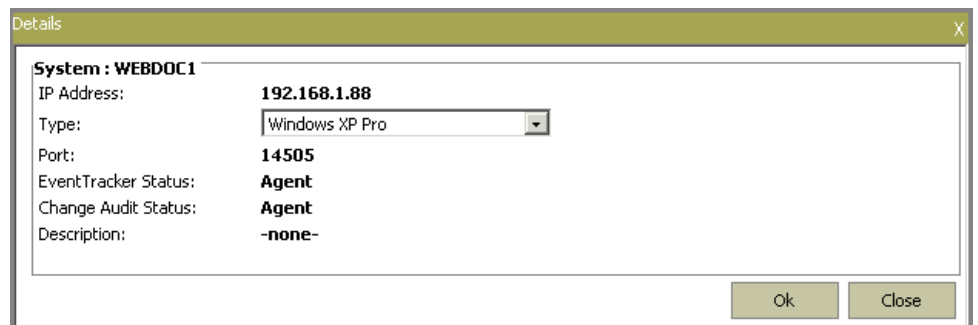
Viewing System Details

This option helps you view system group details and system details like IP address, O/S Type, port, and Agents running on the system.

To view system details

- 1 Open the System Manager.
- 2 To view **system group details**, right-click a system group.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Details**.
System Manager displays the system group Details window.
- 3 To view **managed system details**, move the mouse pointer over a managed system, and then click the dropdown.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Details**.
System Manager displays the system Details window.

Figure 240
System Details



Restarting Agent Service

This option helps to restart EventTracker Windows Agent service in managed systems.

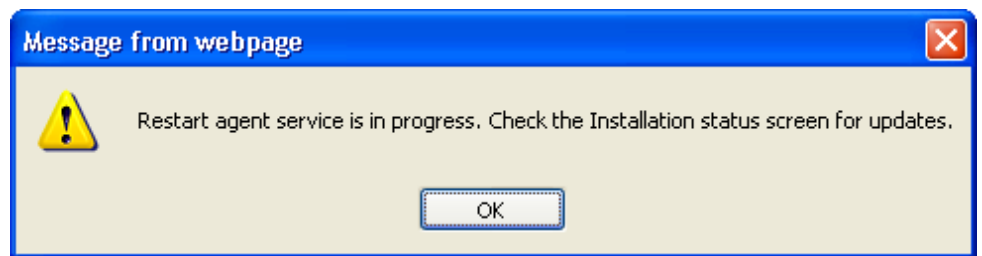
To restart Agent service

- 1 Open the System Manager.
- 2 To restart Agent services in a group, right-click a system group.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Restart agent service**.
- 3 To restart Agent services in a managed system, move the mouse pointer over a managed system, then click the dropdown.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Restart agent service**.
System Manager displays the Restart agent service window.

Figure 241
Restart Agent
Service

- 4 Type valid user credentials and then click **Restart agent service**.
System Manager displays the status of the action.

Figure 242
Status



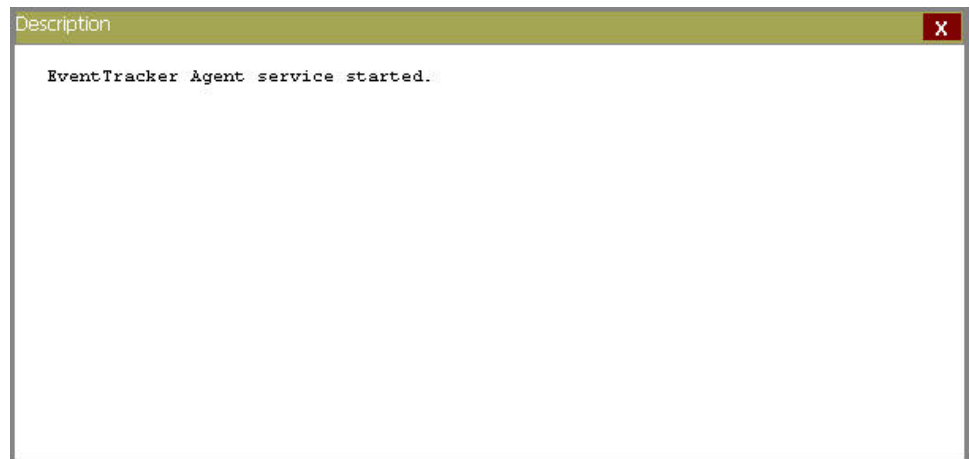
- 5 As advised on the pop-up window, click the **Installation Status** button.
System Manager displays the Installation Status window.

Figure 243
System Status

Installation Status							
Application: All		Status: All		Sort by: Date		Export	
Date	Group/System	By	Agent	Type	Status	Description	
7/16/2010 12:05:19 PM	WEBDOC1	NIRMAL	EventTracker	Restart agent service	Success	view	
7/16/2010 11:29:50 AM	TOONS	NIRMAL	EventTracker	Query for agent version	Success	view	
7/16/2010 11:19:50 AM	WEBDOC1	nirmal	EventTracker	Install agent	Success	Installed successfully.	
7/16/2010 11:19:50 AM	WEBDOC1	nirmal	Change Audit	Install agent	Success	Installed successfully.	
7/16/2010 11:18:41 AM	TOONS,ALL	nirmal	N/A	Search computers	Success	Successfully added group of computers from selected domains.	
7/16/2010 11:18:14 AM	ALL,ALL	nirmal	N/A	Search computers	Success	Successfully added group of computers from selected domains.	

- 6 Click the **View** link in the Description column.
System Manager displays the status of the remote agent.

Figure 244
Description



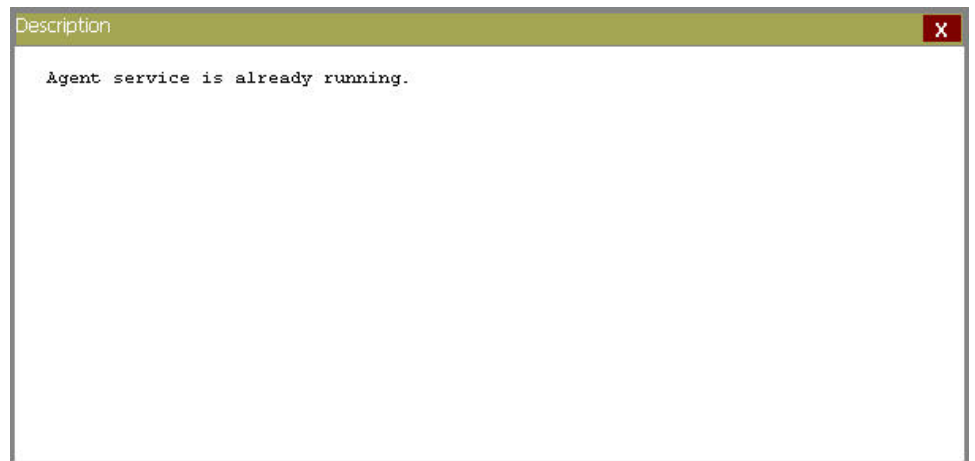
Querying Agent Service Status

This option helps you query EventTracker Windows Agent service status.

To query Agent service status

- 1 Open the System Manager.
- 2 To query Agent service status in a group, right-click a system group.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Agent service status**.
- 3 To query Agent service status in a managed system, move the mouse pointer over a managed system, and then click the dropdown.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Agent service status**.
System Manager displays the Agent service status window.
- 4 Type valid user credentials and then click **Agent service status**.
System Manager displays the status of the action.
- 5 As advised on the pop-up window, click the **Installation Status** button..
System Manager displays the System Status window.
- 6 Click the **View** link in the Description column.
System Manager displays the status of the remote agent.

Figure 245
Description



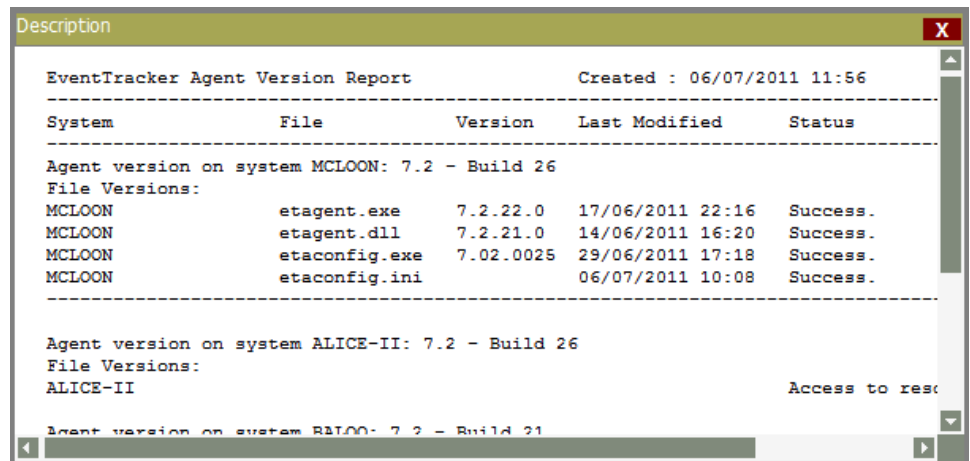
Querying Agent Version

This option helps you query EventTracker Windows Agent version.

To query Agent version

- 1 Open the System Manager.
- 2 To query Agent version in a group, right-click a system group.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Query for agent version**.
- 3 To query Agent version in a managed system, move the mouse pointer over a managed system.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Query for agent version**.
System Manager displays the Query for Agent version window.
- 4 Type valid user credentials and then click **Query for Agent version**.
System Manager displays the status of the action.
- 5 As advised on the pop-up window, click the **Installation Status** button.
System Manager displays the System Status window.
- 6 Click the **View** link in the Description column.
System Manager displays the version of the remote agent.

Figure 246
Description



Managing Asset Value

This option helps you set the asset value of managed systems. Asset Value is the importance or criticality of the computer.

To set asset value

- 1 Move the mouse pointer over the system that you want to set asset value.
System Manager displays the shortcut menu.
From the shortcut menu, choose **Manage Asset value**.
System Manager displays the Manage Asset Value pop-up window.

Figure 247
System Details



- 2 Select the value from the **Asset value** drop-down list.
- 3 Click **Save**.

To set asset value for multiple system in a group

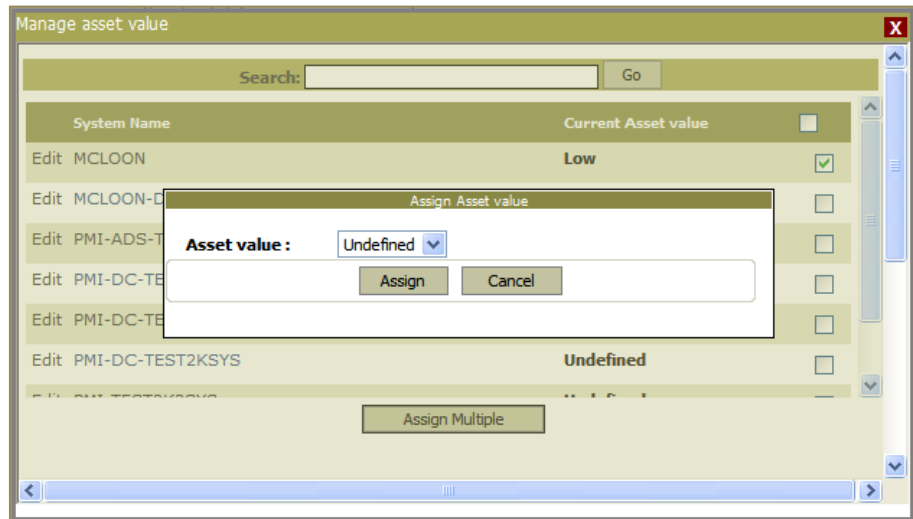
- 1 To set asset value for multiple systems in a group, right-click a system group. System Manager displays the shortcut menu.
- 2 From the shortcut menu, choose **Manage Asset Value**. System Manager displays the Manage Asset Value pop-up window.

Figure 248
Manage Asset Value



- 3 Select **Edit** to change the current asset value of the particular system.
- 4 Select the asset value from the dropdown, and then click **Update**.
- 5 To assign same asset value for multiple systems, select the checkbox for the particular systems, and then click **Assign multiple** button. EventTracker displays Assign Asset Value pop-up window.

Figure 249
Manage Asset Value



- 6 Select the value from the **Asset value** drop-down list, and then click the **Assign** button.

Deleting Systems

This option helps to remove unmanaged systems.

To delete unmanaged systems

- 1 Right-click the system group from where you want to remove the systems.
System Manager displays the shortcut menu.
- 2 From the shortcut menu, click **Delete systems**.
System Manager displays the Delete systems window.

Figure 250
Delete Systems



- 3 Select the system, and then click **Delete**

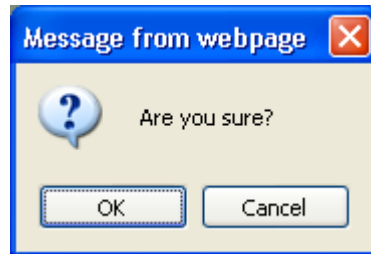
You can select multiple systems by holding CTRL key on your keyboard.

OR

Click the **Check/Uncheck all** checkbox to select all the systems, and then click **Delete** button.

System Manager displays the confirmation message box.

Figure 251
Delete System



- 4 Click **OK** to confirm

System Manager removes the system.

Anytime you add the remove systems. System Manager adds the system under the system group to which it was associated earlier. Refer Manually Adding Computers to add computer manually.

Searching Systems

From the list of all domain computers, this option helps to search system(s) by name.

To search systems

- 1 Type the name of the system in the **Search in list** field.
- 2 Click **Go** button.
EventTracker displays the search result.
- 3 Click **Show All** button to view all systems.

Setting Sort by Option

This option helps to set the sort option.

To set sort order

- Select an option from the **Sort by** drop-down list.
If you select Name, EventTracker displays the system names in alphabetical order.

If you select Asset value, EventTracker displays the system names by priority starting from High.

If you select Port, EventTracker displays the system names with the port number (in descending order) on the top of the list.

Chapter 16

Managing Windows Agents

In this chapter, you will learn how to:

- [Deploy EventTracker Windows & Change Audit Agents](#)
- [View Status](#)
- [Monitor EVTX Log files](#)
- [Enable SID Translation](#)
- [Add USB Exception List](#)
- [Monitor Check Point Logs](#)
- [Monitor VMware Logs](#)
- [Monitor Suspicious Connections](#)
- [Transfer Log Files](#)
- [Assess Configuration](#)

Agent for Windows Systems

As part of the Windows event log management infrastructure, a configurable, high performance, tiny footprint executable (agent) can be deployed to run locally on the managed machine. Usually, the agent is deployed remotely from the System Manager application that is part of EventTracker.

In addition to sending entries from the Event Log, this agent offers many useful features including monitoring application log files, threshold events on CPU/memory/disk utilization, application start/stop, software install/uninstall; service start/stop & runaway processes and monitor TCP/UDP network activities. It can send events with guaranteed delivery (TCP), offers a sophisticated set of filters to limit event transmittal and performs automatic backup and clearing of the Windows Event Log (XP and 2003).

This 'smart' agent offers significantly greater capability over manual log monitoring.

Pros

- **Filters are applied locally** - This minimizes network traffic as insignificant events can be discarded with no further drain on resources.
- **Local agent survives in the face of network failure** - If the Guaranteed Delivery Mode (GED) is used, events are cached and recovered when network recovers.
- **Real time notification** - The agent immediately forwards new local event log entries to the Console. Critical events relating to security, uptime etc usually requires immediate alerts.
- **Performance monitoring** - The agent is capable of detecting excessive CPU, disk or memory usage and reporting it when user defined thresholds are detected.
- **Application monitoring** - The agent is capable of detecting and reporting the start/stop of applications. This can be used to comply with licensing requirements or for usage tracking.
- **Native backup of event logs** - The agent is capable of detecting when the event log is full, backing up the native [.evt](#) file to a configured location and resetting the log. Some installations require the original files (XP and 2003).
- **Software install/removal monitoring** - The agent can detect and report the installation or removal of software from the target machine.
- **Non-domain topology** - The agent needs only a TCP/IP network to communicate with the Console. In particular the Console is not required to be in the same Windows (Active Directory or NT) domain as the agent.
- **Encrypted traffic between Agent and Console** - IPSec techniques can be applied to all traffic between agent and Console for highest security.
- **Service monitoring** - The agent is capable of detecting, reporting, and restarting failed services.

- **Monitoring external log files** – Many applications write a separate log file (e.g. IIS, Antivirus, Oracle etc). New matching entries in such log files can be detected and reported by the agent.
- **Host based intrusion detection** – The agent can detect and report network activity. This is useful as for capacity Flex Report or intrusion detection.

Cons

- **The agent must be installed and configured on the target machine** – This requires planning. Managing product upgrades must also be considered. Deployment and configuration can be done from the Console to minimize this effort.
 - **Possible interaction effects with other software** – Since the agent is an EXE and does get installed on the target machine, there is always a finite probability of negative interaction effects with other software.

The product has operated at many customers in many different environments for many years – so this highly unlikely.
 - **Agent consumes local resources** – The agent, like any application uses some amount of system resources on the target.

The EventTracker agent is highly optimized to absolutely minimize resource usage.
-

Deploying Agents

Pre-installation Procedures

- You MUST have Local Admin privileges on the remote systems where you want to install the Agents.
 - You can also install Agents with Domain Admin privileges.
 - Make sure that the systems that you are selecting to monitor are accessible through the network, have disks that are shared for the Admin, and have disk space up to 50MB that can be used by the Windows Agent.
 - If the remote system is accessed through a slow line, the install may take time and it is recommended that you plan accordingly.
-

Installing EventTracker Windows & Change Audit Agents

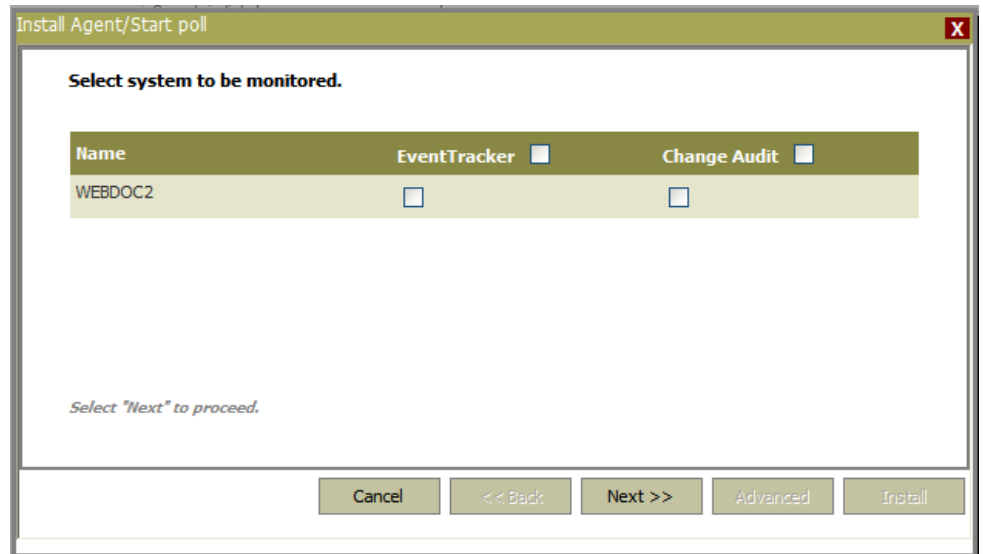
This option enables you to install Windows Agent & Change Audit Agents.

To install EventTracker Window Agent & Change Audit Agent

- 1 Click the Admin dropdown and select Systems.
- 2 EventTracker displays Systems Manager window.

- 3 Click the system where you wish to install the Agent.
System Manager displays the dropdown menu.
- 4 From the dropdown menu, choose **Install agent/ Start Poll**.
System Manager displays the Install Agent/Start Poll window.

Figure 252
Add Agent



- 5 Select the **EventTracker** checkbox to install EventTracker Windows Agent.
and/or
Select the **Change Audit** checkbox to install EventTracker - Change Audit Agent.

Figure 253
Install Agent/Start
Poll – Add Agent

To deploy EventTracker Windows and Change Audit agent on multiple systems:

Click the system group to which the target system is a member.

System Manager displays the shortcut menu.

From the shortcut menu, click **Install agent/Start Poll**.

Name	EventTracker	Change Audit
PMI-ADS-TESTSYS	<input type="checkbox"/>	<input type="checkbox"/>
PMI-DC-TEST2K3SYS	<input type="checkbox"/>	<input type="checkbox"/>
PMI-DC-TEST2K8SYS	<input type="checkbox"/>	<input type="checkbox"/>
PMI-DC-TEST2KSYS	<input type="checkbox"/>	<input type="checkbox"/>
PMI-TEST2K3SYS	<input type="checkbox"/>	<input type="checkbox"/>

1. Select the checkbox next to **EventTracker** and **Change Audit**.

All the systems will be selected and EventTracker Windows and Change Audit agents will get deployed on all managed computers.

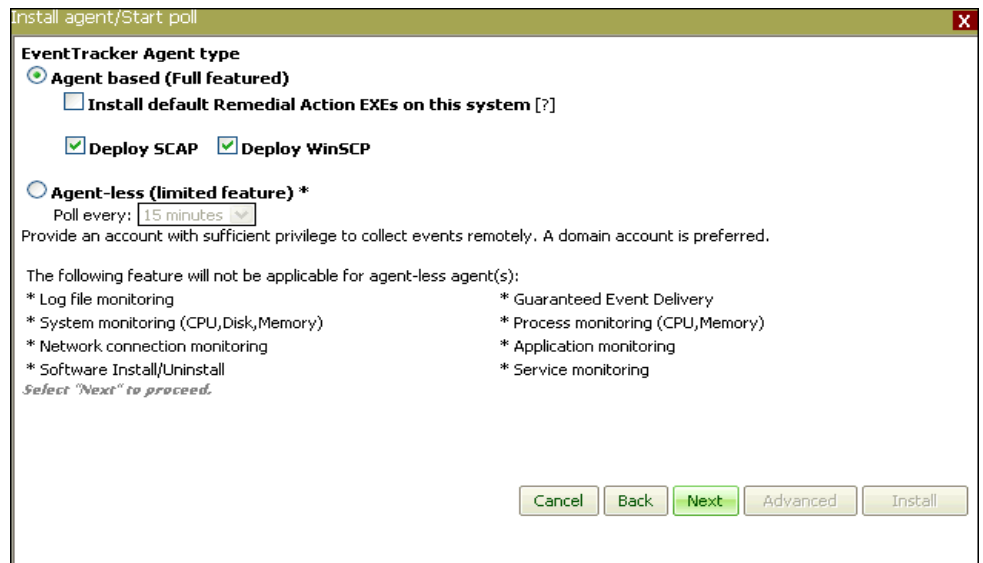
(OR)

Select the respective checkbox next to the system names where you wish to deploy EventTracker Windows and Change Audit agents.

- 6 Click **Next**.

System Manager displays the **Install Agent/Start Poll** window with more options to select.

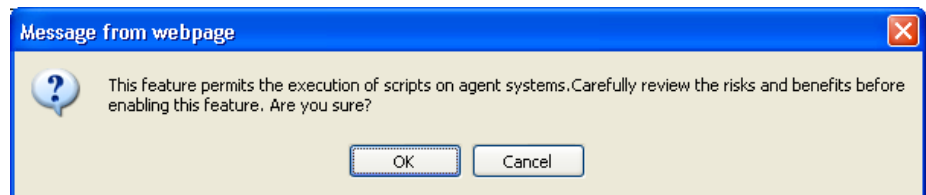
Figure 254



- 7 Click the **Agent based (Full featured)** option, if not selected.
- 8 Click the **Install Remedial Action scripts** checkbox to install the scripts in the EventTracker install directory, typically (... \Program Files \Prism Microsystems \EventTracker \Agent \Script).

System Manager displays the Caution message box. Click **OK** to install scripts.

Figure 255
Remedial Action
Configuration



- 9 Click **Next**.
System Manager displays the Install Agent/Start poll window to provide install path and user credentials.

Figure 255

Click 'Advanced' button to select specific configuration for agent other than the 'Default' configuration.

Install Agent/Start poll

Select installation path on the remote machines:
 (*Valid only for EventTracker agent based monitoring)

☐ Create "Program Menu" shortcuts (*Valid only for EventTracker agent based monitoring)

Account: (ex. mydomain\administrator)
 Password:
 Confirm Password:

Selected systems:
EventTracker [Agent based] :
 WEBDOC2
Change Audit :
 WEBDOC2

Select 'Install' to proceed.

Cancel << Back Next >> **Advanced** Install

- 10 To install the agent in a different drive apart from the default one, type the installation path in the **Select installation path on the remote machines** field.

OR

Type the new path in the **Select Installation path on the remote machines** filed.

Install agent/Start poll

Select installation path on the remote machines:
 (*Valid only for EventTracker agent based monitoring)

☒ Create "Program Menu" shortcuts (*Valid only for EventTracker agent based monitoring)

Account: (ex. mydomain\administrator)
 Password:
 Confirm Password:

Selected systems:
EventTracker [Agent based] :
 DONALD-II

Select 'Install' to proceed.

Cancel Back Next **Advanced** Install

- 11 Click the **Create "Program Menu" shortcuts** checkbox to create shortcut menu on the target system.
- 12 Type valid user credentials.
- 13 Click **Advanced**.

By default, 'Default' configuration will be selected.

Select '**Custom config**' option if you wish to apply custom configuration to the agent. The desired configuration file can be selected from **File** dropdown.

Figure 257
Add Agent – custom
settings

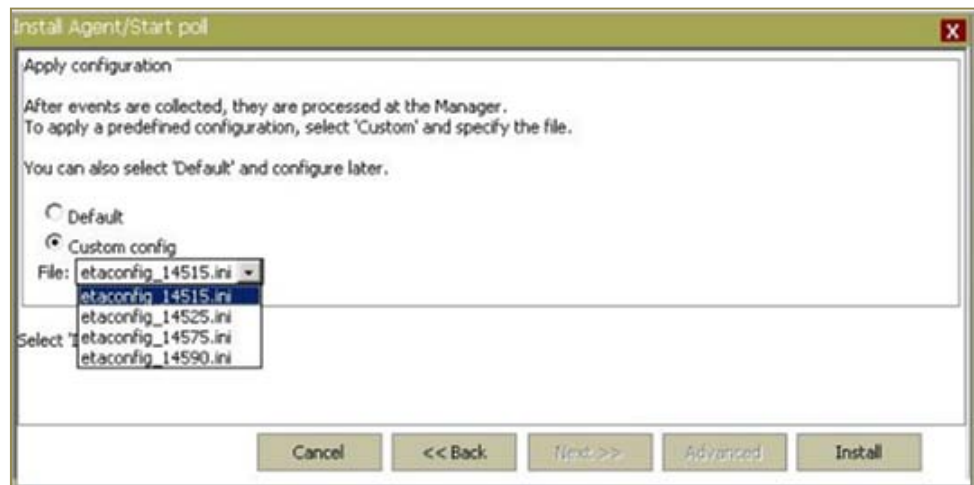


Table 90

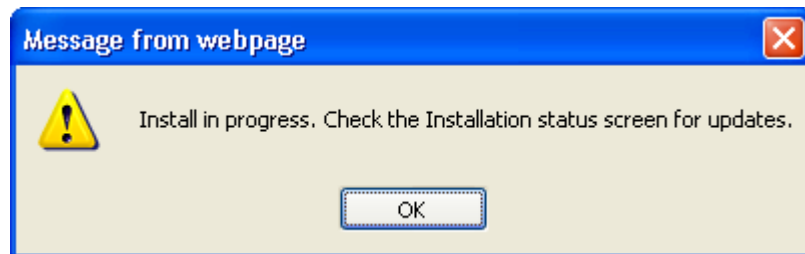
Option	Description
Default	By default, this option is selected for the agent configuration. The default configuration will track all events.
Custom Config	This option is provided to select the custom configuration file. The file extension should be in the EventTracker Agent .ini format and would be a previously saved configuration file. Select the name of the .ini file from the dropdown.

14 Click the appropriate agent configuration settings.

15 Click **Install**.


System Manager starts installing the Agent and displays the message box.

Figure 258
Add Agent –
installation
message



16 Click **OK**.

EventTracker displays Installation Status screen window.

17 Click refresh  to see the updated status.

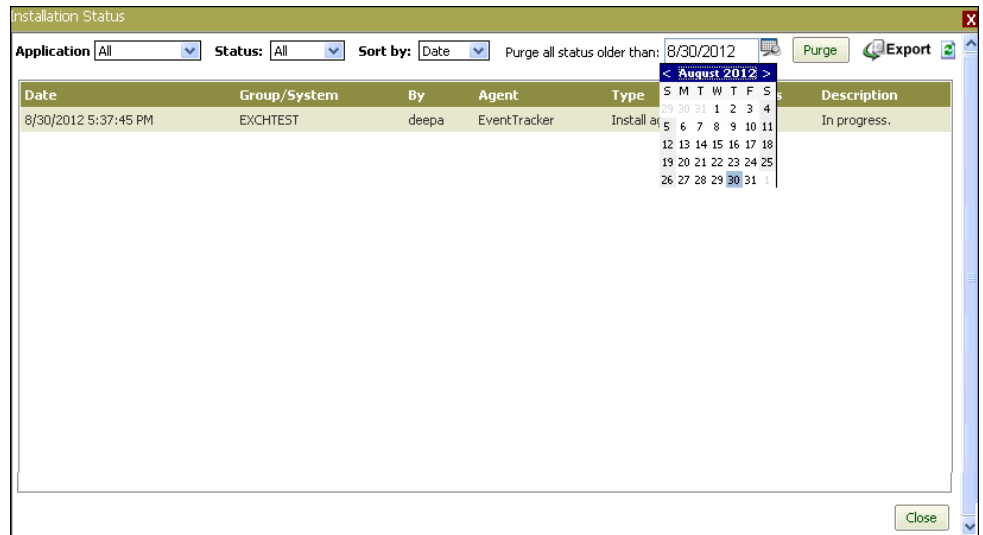
(OR)

Click **Close**.

Click **Installation Status** button.

EventTracker displays Installation Status screen window.

Figure 259
Agent Installation
Status



- 18 Select an option from the **Application** drop-down list to view the installation status of the Agent of your interest.

Available options are EventTracker & Change Audit.

- 19 Select an option from the **Status** drop-down list.

Available options are All, New, Success, and Failed.

- 20 Select an option from the **Sort by** drop-down list.

Available options are Date, System, Type, and Status.

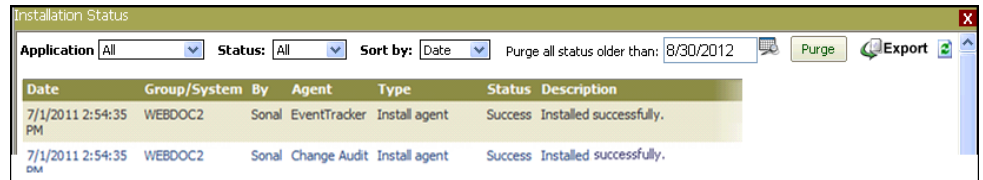
Select **Purge** button it purges the

Purge all status older than drop-down date list.

View System Status

'Installation Status' window helps to view the install/upgrade/uninstall status of EventTracker Windows & Change Audit Agents. You can also view the install status when a computer is added for Agentless monitoring. Other status includes search result when manually discovering and adding computers.

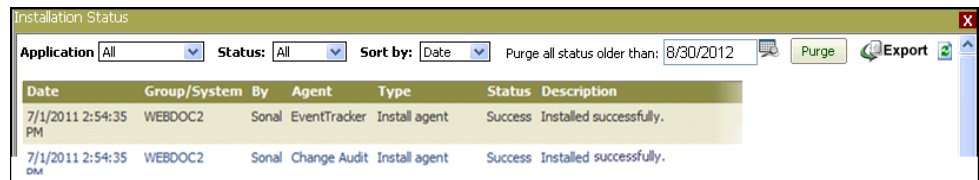
Figure 260
Agent Installation
Status



The screenshot shows a window titled 'Installation Status'. At the top, there are filters: 'Application' set to 'All', 'Status' set to 'All', and 'Sort by' set to 'Date'. To the right, there is a 'Purge all status older than:' field set to '8/30/2012', with 'Purge' and 'Export' buttons. Below the filters is a table with the following data:

Date	Group/System	By	Agent	Type	Status	Description
7/1/2011 2:54:35 PM	WEBDOC2	Sonal	EventTracker	Install agent	Success	Installed successfully.
7/1/2011 2:54:35 PM	WEBDOC2	Sonal	Change Audit	Install agent	Success	Installed successfully.

Figure 261
Agent Installation
Status



This is an identical screenshot to Figure 260, showing the 'Installation Status' window with the same filters and data table.

Table 91

Field	Description
Application	Select the Agent for which you want to view the details.
Status	Select an option to view the status of the agent when a computer is added for Agent based or Agentless monitoring. Available options are All, New, Success, and Failed.
Sort by	This dropdown gives you options like Date, System, Type, and Status to sort the 'Installation status' result set.
Purge	Purges all status older than the current date.

Table 92

Column name	Description
Date	Date and time when the Agent(s) were deployed on the remote computer or added for Agentless monitoring.
Group/System	Name of the group or remote computer to which the agent has been added.
By	Name of the user who added the remote computer for Agent based or Agentless monitoring.
Agent	'EventTracker' indicates that EventTracker Windows Agent was installed on the computer or the computer was added for Agentless monitoring. 'Change Audit' indicates that Change Audit Agent was deployed on the remote computer.
Type	Indicates whether the EventTracker / Change Audit Agent was searched for, installed, removed, or upgraded on the remote computer.
Status	Indicates install/upgrade/uninstall status of EventTracker /

	Change Audit Agent.
Description	<p>Short description of success or failed status of install/upgrade/uninstall status of EventTracker / Change Audit Agent and other.</p> <p>'In Progress"</p> <p>'Installed successfully."</p> <p>'Uninstallation done successfully."</p> <p>'Upgrade done successfully."</p> <p>'EventTracker Agent service started."</p> <p>'EventTracker Agent service already running."</p> <p>'Unknown error. This may be due to insufficient permission or network problems.'" etc.</p>

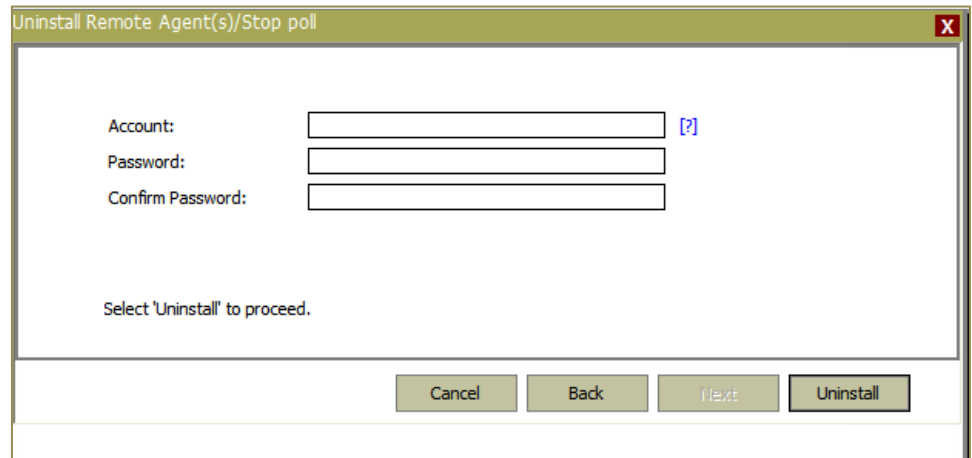
Uninstalling EventTracker Windows & Change Audit Agents

This option enables you to uninstall Windows & Change Audit Agents from the remote computer.

To uninstall EventTracker Windows & Change Audit Agents

- 1 Open the System Manager.
- 2 Move the pointer over the system from where you want to uninstall the agent, and then click the dropdown.
System Manager displays the shortcut menu.
- 3 From the shortcut menu, click **Uninstall agent/Stop Poll**.
System Manager displays the **Uninstall Remote Agent(s)/Stop Poll** window.
- 4 Select the Agent(s) you want to uninstall and then click **Next**.
EventTracker asks for the user credentials of the remote system.

Figure 262
Uninstall Remote
Agent(s)



Uninstall Remote Agent(s)/Stop poll

Account: [?]
 Password:
 Confirm Password:

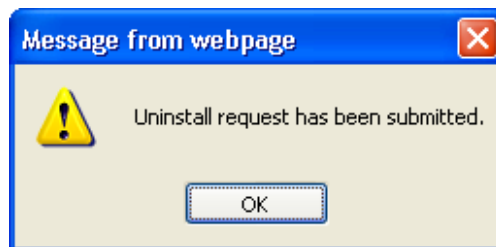
Select 'Uninstall' to proceed.

Cancel Back Next Uninstall

- 5 Type valid user credentials, and then click **Uninstall**.

System Manager starts uninstalling the agent(s) and displays the message box with appropriate message.

Figure 263
Uninstall Remote
Agent(s) –
Successful uninstall
message



- 6 Click **OK**.
 - 7 To view the status of uninstallation, click **Installation Status** button.
- EventTracker displays Installation Status screen.

Figure 264
Installation Status



Installation Status						
Application: All Status: All Sort by: Date						
Date	Group/System	By	Agent	Type	Status	Description
7/1/2011 3:23:24 PM	WEBDOC2	Sonal	EventTracker	Uninstall agent	Success	Uninstallation done successfully.
7/1/2011 3:23:24 PM	WEBDOC2	Sonal	Change Audit	Uninstall agent	Success	Uninstallation done successfully.

Upgrading EventTracker Windows & Change Audit Agents

This option enables you to upgrade EventTracker Windows and Change Audit Agents that are within the domain by selecting 'Windows Domain Network' option and 'Upgrade over IP' option that are outside the domain.

To upgrade EventTracker Windows & Change Audit Agents

- 1 Open the System Manager.
- 2 Move the pointer over the system for which you want to upgrade the agent, and then click the dropdown OR to select more than one system for upgrade, right click the group name.
System Manager displays the shortcut menu.
- 3 From the shortcut menu, click **Upgrade agent**.
System Manager displays the **Upgrade Remote Agent(s)** window.
- 4 Select the Agent(s) you want to upgrade, and then click **Next**.
System Manager displays the Upgrade Remote Agent(s) window with more options.

Figure 265
Upgrade Remote
Agent(s)

Table 93

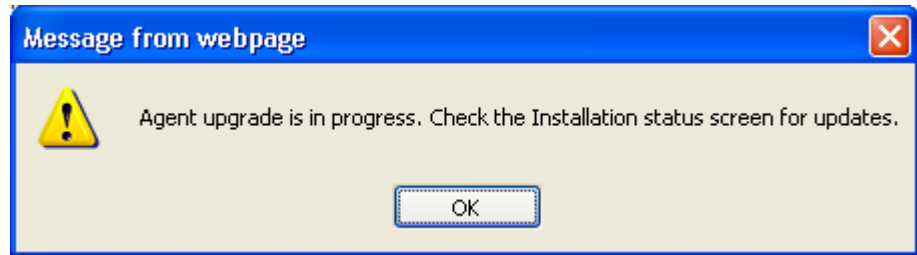
Field	Description
Upgrade Method	
Windows Domain Network	Select this option if all systems to be upgraded can be reached over the Windows Network and you have administrative privileges on all these systems.
Upgrade Over IP (Non Windows)	Select this option if all systems to be upgraded can be reached only via IP and not by the Microsoft Network.

Domain)	
Install default Remedial Action EXEs on this system	Select this checkbox to install remedial executables on this system.

- 5 Select an appropriate Upgrade Method.
- 6 Type valid user credentials and then click **Upgrade**.

System Manager starts upgrading the Agent(s) and displays the message box with appropriate message.

Figure 266
Upgrade Remote
Agent(s)



- 7 Click **OK**.
- EventTracker displays **Installation Status** window.

Note

To apply custom configurations, click **Advanced**.

Removing Windows Agent Components

When the Agents installed on the remote system are removed manually on that system, manager side database will have entries of that system. This option enables you to remove those entries and other remnant components.

To remove Agent components

- 1 Open the System Manager.
- 2 Move the pointer over the system where you wish to remove 'Agent components', and then click the dropdown.

OR

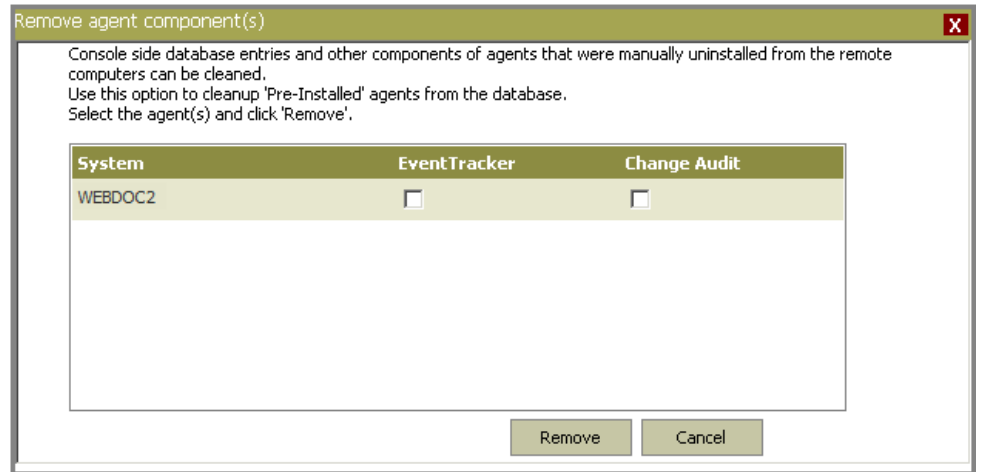
To delete agent component(s) for more than one system, right click the respective group name.

System Manager displays the shortcut menu.

- 3 From the shortcut menu, click **Remove agent components**.

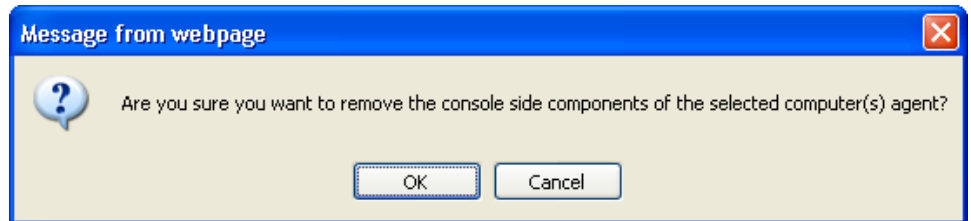
System Manager displays the 'Remove agent component(s)' window.

Figure 267
Remove Agent
Components



- 4 Select the agent to be removed, and then click the **Remove** button
EventTracker displays the confirmation message box.

Figure 268
Remove Agent
Components



- 5 Click **OK** to remove components.

Vista Agent

Event Publishers in Windows Event Log

An event publisher creates an event and delivers it to an event log. An event publisher is typically an application, service, or driver. There can be multiple publishers for large applications, and the publishers should be distinguished by the major components of an application.

Event Logs and Channels in Windows Event Log

A channel is a named stream of events that transports events from an event publisher to an event log file, where an event consumer can get an event. Event channels are intended for specific audiences and have different types for each audience. While most channels are tied to specific event publishers (they are created when publishers are installed and deleted when publishers are uninstalled), there are a few channels that are independent from any event publisher. System

Event Log channels and event logs, such as System, Application, and Security, are installed with the operating system and cannot be deleted.

A channel can be defined on any independent Event Tracing for Windows (ETW) session.

Such channels are not controlled by Windows Event Log, but by the ETW consumer that creates them. Channels defined by event publishers are identified by a name and should be based on the publisher name.

Event Consumers in Windows Event Log

Event consumers are entities that receive events from a computer. Windows Event Viewer (EventVwr.exe) is an event consumer that displays event information from a variety of specified event logs.

There are two types of Windows Event Log consumers:

Subscribers: Applications that receive event notifications as they are received by Windows Event Log.

Event log readers: Applications that query logged events.

[For more details, Log on to Microsoft Web site.](#)

Prerequisites

Following are the mandatory settings you ought to do on Vista systems before you deploy Vista Agent.

- 1 By default, the Startup Type of Remote Registry is manual. Modify the Startup Type as Automatic and Start the service.
 - 2 Enable File and Printer Sharing.
 - 3 Turn on and enable Network Discovery.
 - 4 To configure Vista agent remotely, on Vista system add port no 14503/14506 TCP to Firewall Exceptions.
 - 5 The user must be domain administrator, member of domain admin, or must be added to the local administrator group on the Vista system where the agent has to be deployed.
-

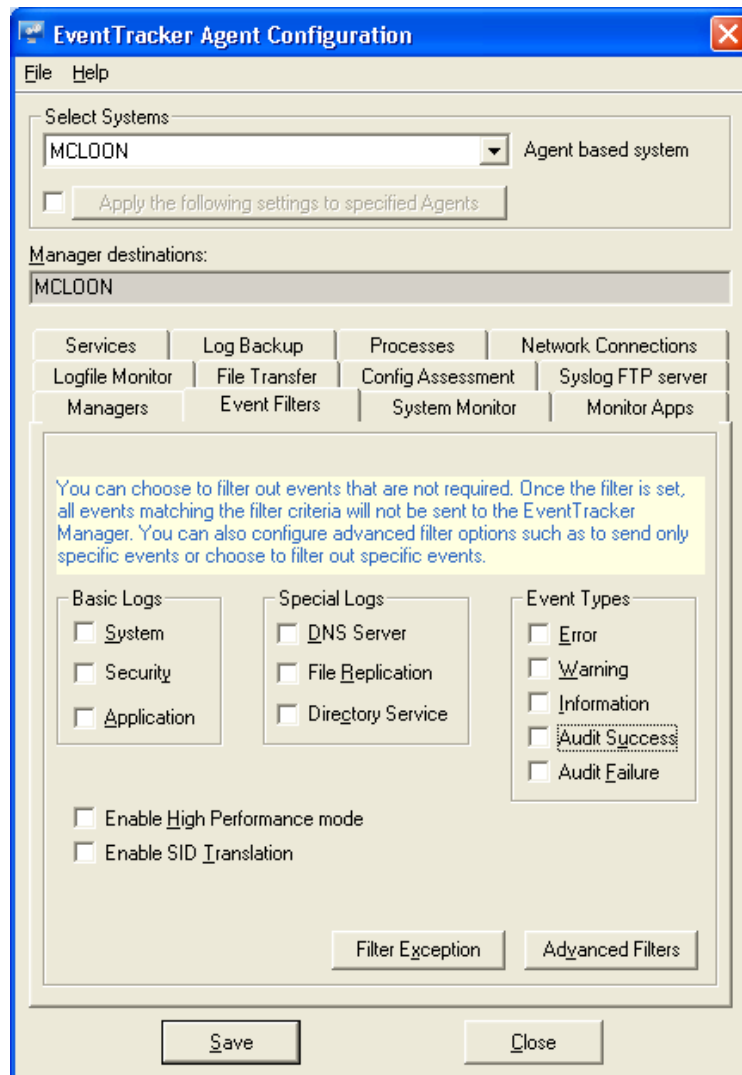
Installing / Uninstalling Vista Agent

Installation and uninstall procedure for Vista Agent is identical to the procedures for other Windows Agents. No other additional configuration settings are required.

Filtering Events

Event Logs is a dynamic list of Channels. Whenever a new Channel is provided for subscription, EventTracker updates this list automatically. High performance mode is not available for Vista Agent.

Figure 269
Vista Agent
Configuration
window – Event
Filters tab



Monitoring EVTX Logfiles

This option enables you to monitor Vista event log back up files.

To monitor EVTX log files

- 1 Go to EventTracker Control Panel and click on the EventTracker Agent Configuration icon.
- 2 Select the system from the **Select Systems** drop-down list.
- 3 Click the **Logfile Monitor** tab.

EventTracker displays the Logfile Monitor tab.

4 Click **Add File Name**.

EventTracker displays the Enter File Name dialog box.

5 Select the logfile type as **EVT** from the **Select Logfile Type** drop-down list.

6 Type the path in the **Enter File Name** field (OR) click  to locate and select the log file.

EventTracker displays the Select Folder/File Name dialog box.

7 Go to the appropriate folder and then select the file.

8 Click **OK**.

9 Select the log type from the **EVT Log Type** drop-down list.

10 Click **OK**.

EventTracker displays the Agent Configuration window with newly added configuration settings.

11 Click **Save**.

Configuring Windows Agent

EventTracker Manager automatically backs up recent configuration files (etaconfig.ini & spmConfig.ini) of local and remote Agents in a centralized location on the Manager system.

...\\Program Files\\Prism Microsystems\\EventTracker\\AgentConfig

For example: The naming convention would be

etaconfig.ini.ESXWEBDOC

spmConfig.ini.ESXWEBDOC

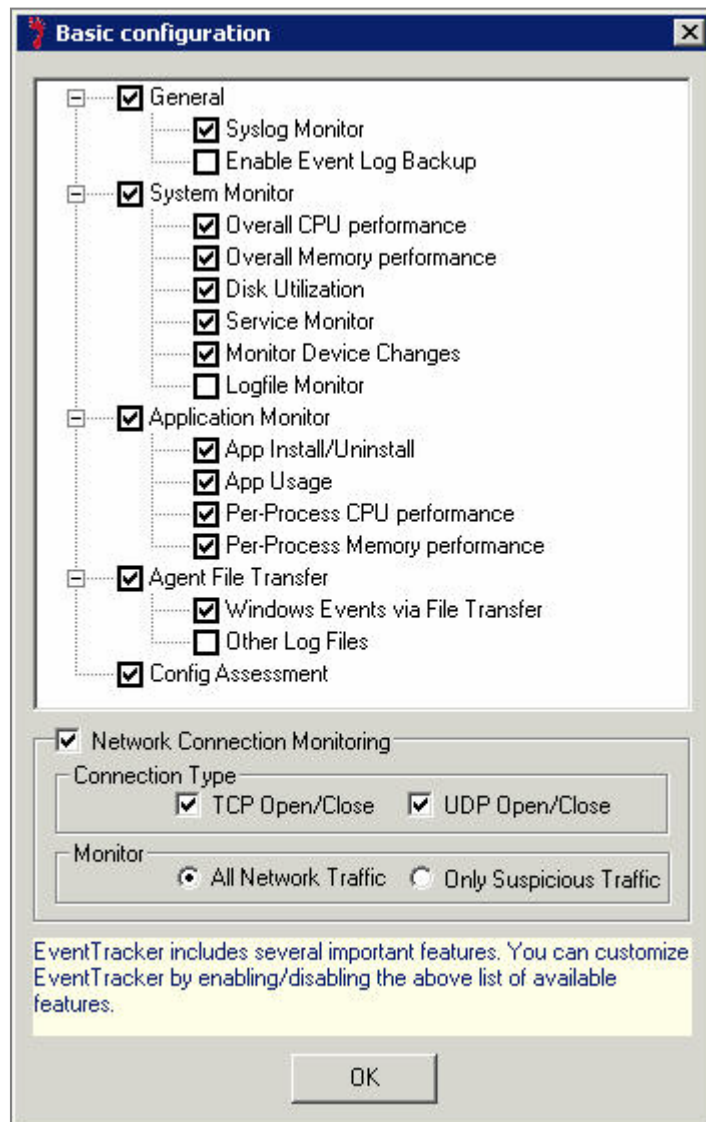
etaconfig.ini.WEBDOC1

spmConfig.ini.WEBDOC1

Basic Configuration

While installing EventTracker, you have the liberty to set the basic configuration settings.

Figure 270
Basic configuration
settings



- Select appropriately, and then click **OK**. You can also configure the monitoring options through the 'Agent Configuration' window after installing EventTracker.

Forwarding Events to Multiple Destinations

This option enables you to configure windows agent to simultaneously report log events or syslog events to more than one manager.

To configure Windows Agent to forward Events to multiple managers

- 1 Log on to EventTracker Enterprise.

- 2 Click the **Admin** dropdown at the upper-right corner, and then click **Windows Agent Config**.

EventTracker displays the 'Windows Agent Configuration' page.

Figure 271
Windows Agent
Configuration

- 3 Click **Select System** hyperlink to select the system.
EventTracker displays **Agent Systems** pop-up window.

Figure 272
Agent System

EventTracker displays the error messages, if the client is not running on the selected system, or may have older version or the client could not be contacted.

- 4 Click the system name on which you wish to forward the events.

- 5 Click the **Managers** tab, if not selected.
 - 6 In 'EventTracker Managers' pane, click **Add**.
- EventTracker displays the **Add Destination** pop-up window.

Figure 273
Add Destination
window

Table 94

Field	Description
Destination	Type the system name in this field. Make sure that EventTracker Manager is installed on this system.
Resolve	Identifies given IP address or system name and check its availability in the network. Displays an error message on entering wrong IP address or system name.
Port	Type the port number in this field. By default, the port number is 14505.
Connect to Manager using	Select the appropriate option. The options are High Performance Mode (UDP) and Guaranteed Delivery Mode (TCP).
Encrypt	Select an option to encrypt or not the data that flows from the Agent to the Manager.
Configure cache folder	Select the cache folder. This is used to store events locally on the Agent system when the connection to EventTracker Manager is lost.
Minimum Amount of Free space to be	This is the feature applies to TCP mode of agent. Actual usage of TCP mode is to deliver the event in a guaranteed

Field	Description
left on Storage Device (%)	<p>way irrespective of connection problems, Receiver status etc. In case if the Agent is not able to communicate with the Receiver, Agent will start storing all the events as cache files in the specified folder (refer: Configure cache folder).</p> <p>If the Receiver is dead for weeks together, Agent keeps storing these files in disk and there by affecting DISK SPACE on critical systems.</p> <p>To control this problem, the option "Minimum Amount of Free space to be left on Storage Device(%)" is provided to stop storing events when the disk space is less than the configured number of %.</p> <p>Example, when you configure 20%, Agent will stop writing events to disk when the free space goes down beyond 20%.</p> <p>All these apply only to TCP mode.</p>

- 7 Enter/select appropriately in the relevant fields.
- 8 Click **OK**.
- 9 Click **Save**.

To configure Windows Agent to forward syslog Events to different managers

- 1 Open EventTracker Control panel.
- 2 Double click **EventTracker Agent Configuration**.
EventTracker displays EventTracker Agent Configuration window.
- 3 Select the system from **Select Systems** dropdown to which you wish to forward the syslog events.
EventTracker may display the error message (as below), if the client is not running on the selected system, or may have older version or the client could not be contacted.

Figure 274
Error message



- 4 Click the **Managers** tab, if not selected.
- 5 In Syslog Manager(s) pane, click **Add**.
EventTracker displays the **Add Destination** pop-up window.

Figure 275
Syslog- Add
Destination

Add Destination

Destination:

Port:

Connect to Manager using

High Performance Mode uses minimal network traffic (UDP) and is the best choice for most installations.

☒ High Performance Mode (UDP)

☐ Guaranteed Delivery Mode (TCP)

Encrypt:

☒ Authentication

Certificate File:

Certificate Common Name:

Password:

Event cache folder:

Minimum Amount of Free space to be left on Storage Device (%):

OK Cancel

- 6 Click TCP or UDP as the appropriate event delivery mode.
By default, syslog selects UDP option.
- 7 Enter/select appropriately in the relevant fields.
- 8 Click **OK**.
- 9 Click **Save**.

Event Delivery Modes

EventTracker Agents send the event logs garnered to the Manager, either in High Performance mode (UDP) or in Guaranteed Delivery Mode (TCP).

Since UDP is a connectionless network service, there is no guarantee that the Manager will receive all the data blocks transported by the UDP.

In TCP mode, is a connection oriented network service, there is a guarantee that the Manager will receive all the data packets transported by the TCP.

Modifying Event Delivery Modes

This option helps you modify event delivery modes.

To modify Event delivery mode

- 1 Move to the **Windows Agent Configuration** page.
- 2 Click **Select System** hyperlink to select the system.
- 3 Select the Manager that you want to edit.
- 4 In EventTracker Managers pane, click **Edit**.

EventTracker displays the 'Edit Destination' pop-up window.

Figure 276
Edit Destination
window

By default, EventTracker selects the High Performance Mode (UDP) option.

- 5 Select the **Guaranteed Delivery Mode (TCP)** option.

Figure 277
Edit Destination
window

By default, EventTracker stores the cache in the [C:\Program Files\Prism Microsystems\EventTracker\Agent\ged](#) folder. You can also modify, if you prefer a different folder to store cache.

- 6 Type the path of the cache folder in the **Configure cache folder** field.
- 7 Set **Minimum Amount of Free space to be left on Storage Device (%)**.
- 8 Click **OK**.
- 9 Click **Save**.

Modifying Event Delivery Modes for Syslog

By default, Syslog selects **High Performance Mode (UDP)** option. If you wish to select Guaranteed Delivery - TCP mode option then,

- 1 In the '**Syslog destinations**' pane, select the manager you wish to edit, and then click the **Edit** button.
EventTracker displays the 'Edit destinations' pop-up window.
- 2 Click the **Guaranteed Delivery Mode (TCP)** option.
- 1 Select encryption option 'YES' from **Encrypt** dropdown.
- 2 Click **Authentication** checkbox.
- 3 Enter or browse the certificate file name.

This Certificate file contains personal information exchange (PFX) standard for signing or encrypting data.

- 4 Enter name of the certificate in **Certificate Common Name** field.
 - 5 Enter correct password, which is used to protect the certificate in the **Password** field.
 - 6 Type the path of the cache folder in the **Configure cache folder** field.
By default, EventTracker stores the cache in the [C:\Program Files\Prism Microsystems\EventTracker\Agent\ged](#) folder.
You can modify the default path, if you prefer a different folder to store the cache.
 - 7 Set the minimum amount of free space to be left on storage device in **Minimum amount of free space to be left on storage device (%)** field.
 - 8 Click **OK**.
 - 9 Click **Save** on the EventTracker Agent Configuration window.
-

Removing Managers

This option helps you remove Managers.

To remove Managers

- 1 Move to the 'Windows Agent Configuration' page.
 - 2 Select the system from the **Select System** hyperlink.
 - 3 Select the Manager that you want to remove.
 - 4 In EventTracker Managers pane, click **Remove**.
 - 5 Click **Save**.
-

Saving Agent configuration

This new option leads you to save the customized manager configuration as Template, in order to use the same configuration settings for other agent systems. The template will be saved as [.ini](#) file in the default path, which would be

[...ProgramFiles\PrismMicrosystems\EventTracker\RemoteInstaller](#)

To Save Configuration

- 1 In EventTracker Enterprise, go to 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Make the required configuration changes in Windows agent configuration page, and then click the **Save** button.
EventTracker saves the configuration for the selected system.
- 4 In order to use the same settings for multiple agent systems, click the **Save as** button to save the setting as template.

EventTracker displays **Template file location** pop-up window.

Figure 278
Save template

- 5 Enter the template name, and then click the **Save** button.

EventTracker saves the agent configuration template in the path specified in **File Location** field.

Note

Default template file location path cannot be changed.

To Modify Template Configuration

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Click the **Load Template** button.

EventTracker displays **Template File location** pop-up window.

Figure 279
Template file
location

- 3 Click the **File name** dropdown to see the configuration template list.
- 4 Select the template file to be modified, and then click the **Load** button.
EventTracker displays configuration settings of the selected template file.
- 5 Make the required changes in the template configuration.
- 6 Click **Save as** button to save the configuration changes in different template file.
(OR)

Click **Save** button to save the configuration changes in the same Template file.

To Apply Configuration to system(s)

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Click the **Load Template** button, select the **File name**, and then click the **Load** button.

Windows Configuration manager page, displays the selected template configuration.

Figure 280
Windows
configuration page

Selected template name: [Select system](#)

Manager Destinations:

Managers

License server: Port:

Upto 5 managers can be configured.

EventTracker Managers

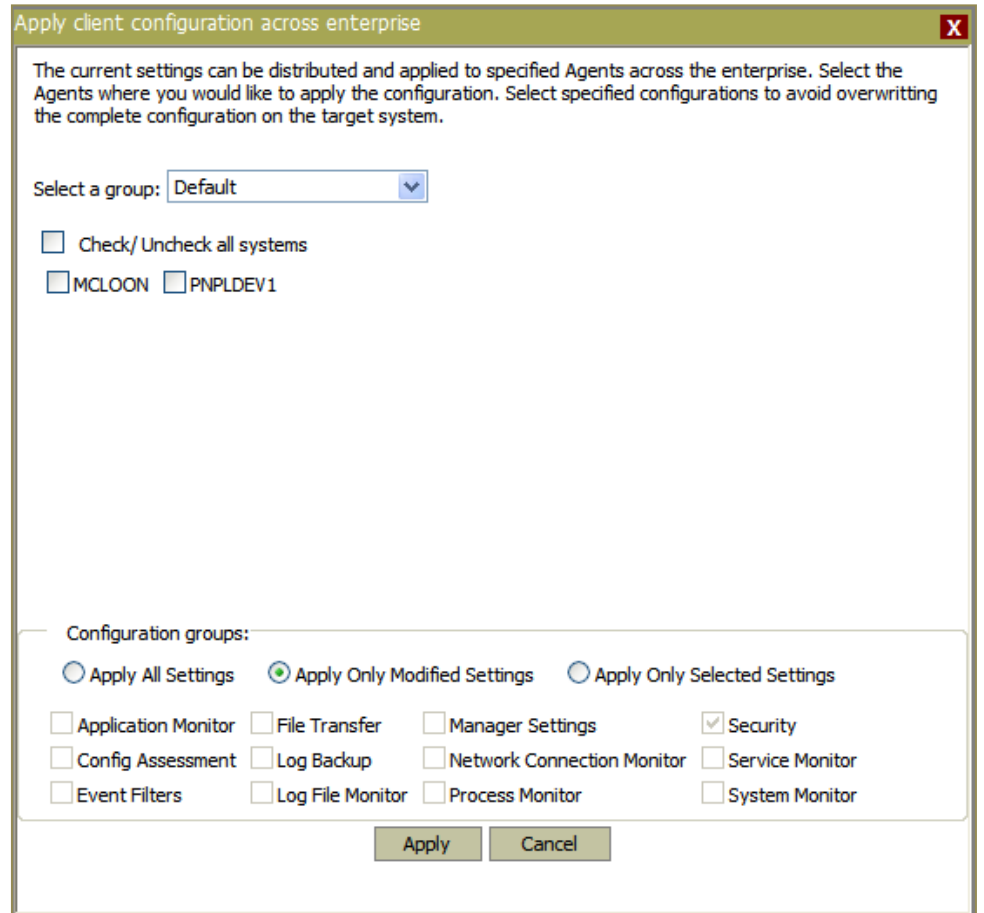
Manager Name	Port	Delivery Mode	Encrypt
MCLOON	14505	UDP	No

Syslog destinations

Manager Name	Port	Delivery Mode	Encrypt
--------------	------	---------------	---------

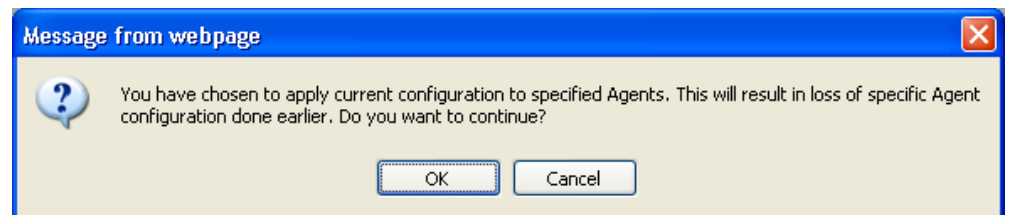
- 3 Click **Apply this configuration to agents** button.
EventTracker displays a pop-up window.

Figure 281 Client Configuration



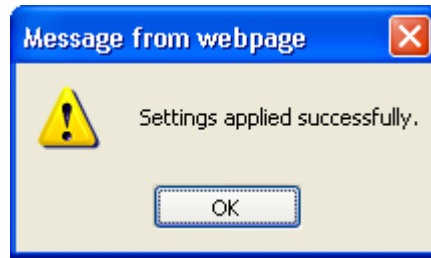
- 4 Select system(s) and required settings from **Configuration groups** pane.
 - 5 Click the **Apply** button.
- EventTracker displays a warning message.

Figure 282



- 6 Click the **Ok** button.
- EventTracker displays confirmation message.

Figure 283



- 7 Click the **Ok** button.

The template configuration loaded successfully on the selected systems.

Note

You can use configuration files to apply the custom configuration to the single/multiple system. This can be done while installing or upgrading the agent(s) through system manager in EventTracker web console.

Filtering Events

This option enables you to filter events being sent to the Manager. Select appropriate checkboxes under Basic Logs, Special Logs, and Event Types.

To filter events

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Event Filters** tab.

EventTracker displays the Event Filters tab.

Figure 284
Agent Configuration
window – Event
Filters tab

Table 95

Field	Description
Basic Logs	Select appropriate checkboxes to filter the events being sent to the Manager.
Special Logs	Select appropriate checkboxes to filter the events being sent to the Manager.
Event Types	Select appropriate checkboxes to filter the events being sent to the Manager. Example: Event Types -> Warning The filter is now set and all events with Event Type Warning will be filtered out and will not be sent to EventTracker Manager.
Enable SID Translation	Select this checkbox to enable SID translation. For more information on SID translation, refer SID-translate.pdf in the EventTracker installation folder.
Enable High Performance mode	Select this checkbox to switch the Agent performance modes.
Filter Exception	Click this button to set the filter exceptions for the specific events that you want to monitor.
Advanced Filters	Click this button to set the filters for the specific events that you do not want to monitor.

By default, EventTracker filters Information and Audit Success events.

4 Set the available filter options appropriately, and then click the **Save** button.

Filtering Events with Exception

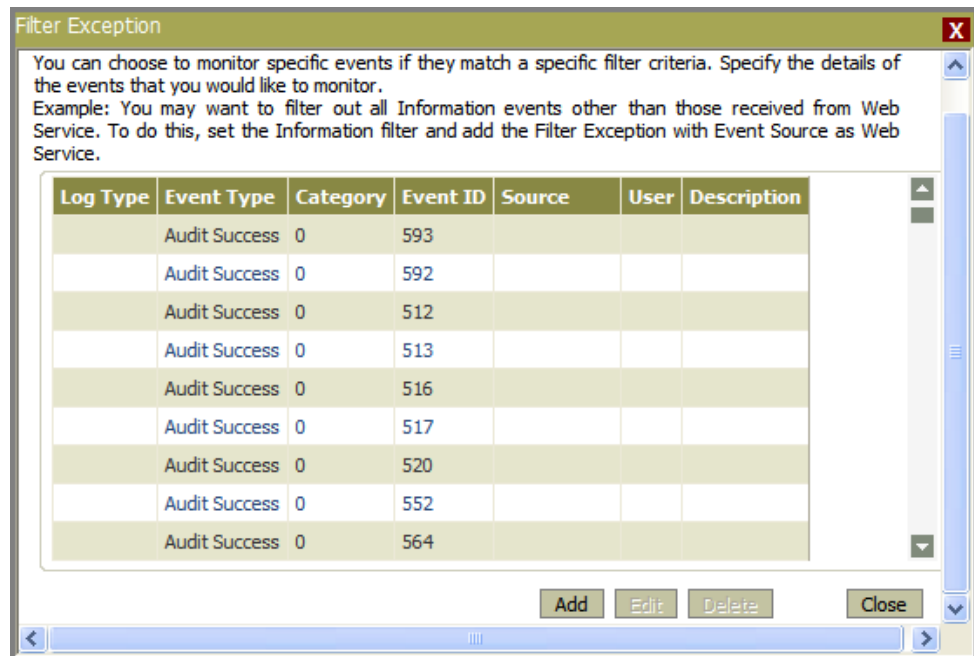
This option helps you to filter events with exception. For example, had you configured agent to filter **Information** events, all events of 'Information' event type will not be forwarded to the Manager. However, if you wish to send specific events of **Information** event type, you can exempt those events from filtering.

To filter events with exceptions

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Event Filters** tab.
- 4 Click **Filter Exception**.

EventTracker displays the Filter Exception pop-up window with a list of events exempted from filtering.

Figure 285
Filter Exception



- 5 To modify event details, select a row and then click **Edit**.
- 6 To remove event details, select a row and then click **Delete**.
- 7 To add filter exceptions, click **Add**.

EventTracker displays the Filter Exception pop-up window to select/enter event details.

Figure 286
Filter Exception

Filter Exception

Event Details (empty field implies all matches)

Log Type : [dropdown]

Event Type : [dropdown]

Event Id : [text]

Category : [text]

Match in User : [text]

Match in Source : [text]

Match in Event Description : [text]

"Match in Event Description" field can take multiple strings separated with && or ||.
 -&& stands for AND condition
 -|| stands for OR condition
 Note:
 If you want to make a match on any of the special characters like, "\", "^", "&", etc...
 then in the search string prefix this
 Example: "\\" for a "\" and "\\^" for a "^"
[For more information click here](#)

Ok Cancel

8 Type appropriately in the relevant fields.

Figure 287
Event Details
window

Filter Exception

Event Details (empty field implies all matches)

Log Type : [dropdown]

Event Type : Information [dropdown]

Event Id : [text]

Category : [text]

Match in User : [text]

Match in Source : Web Service [text]

Match in Event Description : [text]

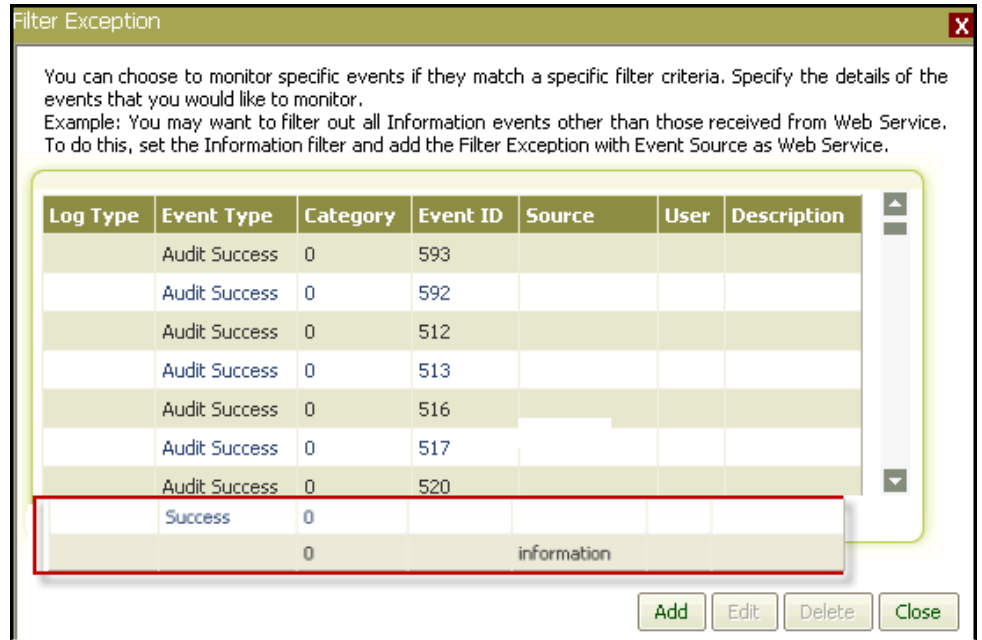
"Match in Event Description" field can take multiple strings separated with && or ||.
 -&& stands for AND condition
 -|| stands for OR condition
 Note:
 If you want to make a match on any of the special characters like, "\", "^", "&", etc...
 then in the search string prefix this
 Example: "\\" for a "\" and "\\^" for a "^"
[For more information click here](#)

Ok Cancel

9 Click **OK**.

EventTracker displays the Filter Exception pop-up window with the newly added filter exception.

Figure 288
Filter Exception
window



10 Click **Close**.

11 Click **Save**.

Filtering Events with Advanced Filters

Filters and Filter Exception go hand in hand, which means you can filter all the events but with exceptions. Whereas Advanced Filters help, you filter out a specific event allowing other events of that type.

To filter events with Advanced Filters

- 1 Move to the Windows Agent Configuration page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Event Filters** tab.
- 4 Click **Advanced Filters**.

EventTracker displays the **Advanced Filters** pop-up window with a list of advanced filters.

Figure 289
Advanced Filters
window

Advanced Filters

You can choose NOT to send specific events. Specify the details of the events which you would like to ignore.
Example: You may want to view all the information events other than those received from FTP Service. To do this, add a specific event with Event Source as FTP Service.

Log Type	Event Type	Category	Event ID	Source	User	Description
	0	0	0		ANONYMOUS USER	
	0	0	0		ANONYMOUS LOGON	
Security	0	0	578		\$	
Security	0	0	540		\$	
Security	0	0	538		\$	
Security	0	0	528		\$	

Add
Edit
Delete
Close

5 Click **Add**.

EventTracker displays the Advanced Filters pop-up window to select/enter event details.

6 Type appropriately in the relevant fields.

Figure 290
Advanced Filters
window

Advanced Filters

Event Details (empty field implies all matches)

Log Type : [Dropdown]

Event Type : [Error]

Event Id : [Text Box]

Category : [Text Box]

Match in User : [Text Box]

Match in Source : [Symantec Antivirus]

Match in Event Description : [SYMANTEC TAMPER]

"Match in Event Description" field can take multiple strings separated with && or ||.
 -&& stands for AND condition
 -|| stands for OR condition
 Note:
 If you want to make a match on any of the special characters like, "\", "^", "&", etc...
 then in the search string prefix this
 Example: "\\" for a "\" and "\\^" for a "^"
[For more information click here](#)

Ok Cancel

7 Click **OK**.

EventTracker displays the Advanced Filters pop-up window with the newly added filter.

Figure 291
Advanced Filters
window

Advanced Filters

You can choose NOT to send specific events. Specify the details of the events which you would like to ignore.
 Example: You may want to view all the information events other than those received from FTP Service. To do this, add a specific event with Event Source as FTP Service.

Log Type	Event Type	Category	Event ID	Source	User	Description
	0	0			ANONYMOUS LOGON	
Security	0	0	578		\$	
Security	0	0	540		\$	
Security	0	0	538		\$	
Security	0	0	528		\$	
Error	0	0		Symantec Antivirus		SYMANTEC TAMPER

Add Edit Delete Close

8 Click **Close**.

 **Note**

The filter is set and specific events matching the filter criteria will not be forwarded to EventTracker Manager. All Error Events will be forwarded to the Manager except the events matching the filtered criteria set.

- 9 Click **Save**.

Enabling High Performance Mode

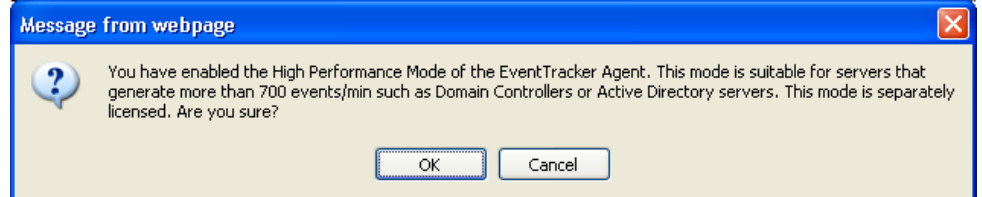
This option helps you enable High Performance mode.

To enable High Performance mode

- 1 Move to the Windows Agent Configuration page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Event Filters** tab.
- 4 Select the **Enable High Performance mode** checkbox.

EventTracker displays the caution message box.

Figure 292
EventTracker Agent
Configuration
message box



- 5 Click **OK**.
- 6 Click **Save**.

Enabling SID Translation

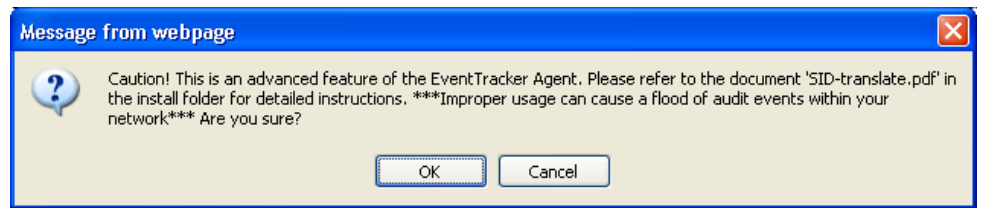
This option helps you enable SID translation.

To enable SID translation

- 1 Move to the Windows Agent Configuration page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Event Filters** tab.
- 4 Select the **Enable SID Translation** checkbox.

EventTracker displays the Caution message box.

Figure 293
EventTracker Agent
Configuration
message box



- 5 Click **OK**.
- 6 Click **Save**.

Note

This feature works in all versions of EventTracker from 5.2 upwards. More information please go through SID-translate.pdf found in the EventTracker installation folder typically, ...\\Program Files\\Prism Microsystems\\EventTracker.

Monitoring System Health

Monitoring CPU, memory performance and disk usage of a system enables the administrator to monitor the general health of a system. You can configure general health thresholds for CPU and Memory Usage. All thresholds are measured in percent terms.

When the configured threshold is crossed, an event will be generated and reported to the manager. An event will also be generated when the thresholds are back to below configured levels.

Care is taken not to report spikes in CPU or memory usage by a process. Therefore, when an event is seen that a system is crossing thresholds, you can be sure that this is for a long enough period and need to investigate.

The default threshold limits are 80% for all variables. A configuration of 0% would disable the monitoring for that specific variable.

USB and other Device Changes option helps to monitor insertion or removal of USB and other media. Also helps to track file transactions that occur in the inserted media.

To configure system performance thresholds

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **System Monitor** tab.

EventTracker displays the System Monitor tab.

Figure 294
System Monitor tab

Table 96

Field	Description
Performance	
CPU Performance (%)	Select a threshold limit to monitor CPU performance from the drop-down list.
Memory Usage (%)	Select a threshold limit to monitor memory usage from the drop-down list.
Disk Space Usage (%)	Select a threshold limit to monitor disk space usage from the drop-down list.
USB and other Device Changes	
Report insert/remove	Select this checkbox to track insertion or removal of USB or other devices. This checkbox is selected by default.
Record activity	Select this checkbox to monitor file transactions occur in the inserted devices.
Disable USB Devices	Select this checkbox to disable USB devices. The selection will enable the 'USB Exception List' button.
USB Exception List	Click this button to add the USB device ID or serial number in the exception list. The listed USB devices will not be disabled when inserted.

- 4 Set the thresholds appropriately.
- 5 Set the tracking and monitoring options.
- 6 Click **Save**.

Adding USB Device in the Exception List

While disabling USB Devices on a particular computer, you can also exempt and enable USB devices from monitoring.

To configure USB exception list

- 1 Select the **Disable USB Devices** checkbox.
- 2 Click **USB Exception List** button.

EventTracker displays the 'USB Exception List' pop-up window.

Figure 295
USB Exception List

The screenshot shows the 'USB Exception List' dialog box. It has a title bar with the text 'USB Exception List' and a close button (X). The dialog is divided into two main sections. The first section is titled 'USB Serial Numbers(Decimal/Hexadecimal format)' and contains the text 'USB devices with the following serial numbers will not be disabled when inserted.' Below this is a large empty text area. Underneath the text area is a label 'Enter USB Serial Number:' followed by a text input field. To the right of the input field are two radio buttons labeled 'Dec' and 'Hex' under the heading 'Format'. Below these are three buttons: 'Add', 'Edit', and 'Remove'. The second section is titled 'Device identifiers' and contains the text 'USB devices with following device identifiers will not be disabled when inserted.' Below this is another large empty text area. Underneath is a label 'Enter USB Device Id:' followed by a text input field. To the right of the input field are three buttons: 'Add', 'Edit', and 'Remove'. At the bottom of the dialog are two buttons: 'Cancel' and 'Save & Close'.

- 3 Type the USB serial number in decimal format or hexadecimal format in the **Enter USB Serial Number** field, and then select the **Format** option accordingly.

OR

Type USB device ID in the **Enter USB Device ID** field.

- 4 Click the **Add** button.

EventTracker adds the newly entered serial number or device Id in the exception list.

- 5 Click **Save & Close** button.

- 6 In 'Windows Agent Configuration' page, click the **Save** button to save the configuration changes.

Note

Please refer [EventTracker-Removable media device monitoring](#) document for more details on creating exception list and its functionality.

Monitoring Applications

This option enables you to monitor installation and un-installation of applications, and monitor application usage.

EventTracker logs a custom information event whenever a monitored application is opened or closed. These events are received at the Console and helps in tracking the application usage.

EventTracker monitors all applications specified in 'Monitor Specific Apps' and ignores applications specified in 'App Exception'.

To monitor application installation and un-installation

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Application Monitor** tab.

EventTracker displays the 'Application Monitor' tab.

Figure 296
Application Monitor
tab

The 'Monitor Specific Apps' takes precedence over 'App Exceptions'. Hence, if an application is specified in both the sections then it will be monitored.

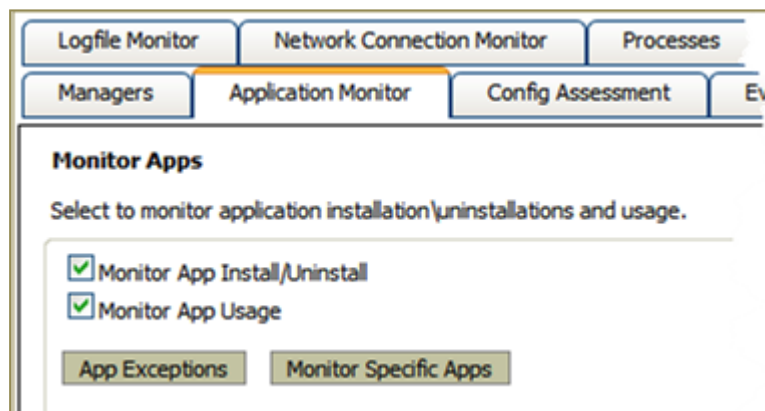


Table 97

Field	Description
Monitor App Install/ Uninstall	Select this checkbox to monitor installation and un-installation of applications.
Monitor App Usage	Select this checkbox to monitor application usage. This selection enables the App Exceptions and Monitor Specific Apps buttons.
App Exceptions	Enables you to set the applications that you do not wish to monitor.
Monitor Specific Apps.	Enables you to set the applications that you wish to monitor.

- 4 Select appropriately the **Monitor App Install / Uninstall** and **Monitor App Usage** options.
- 5 Click the **Save** button.

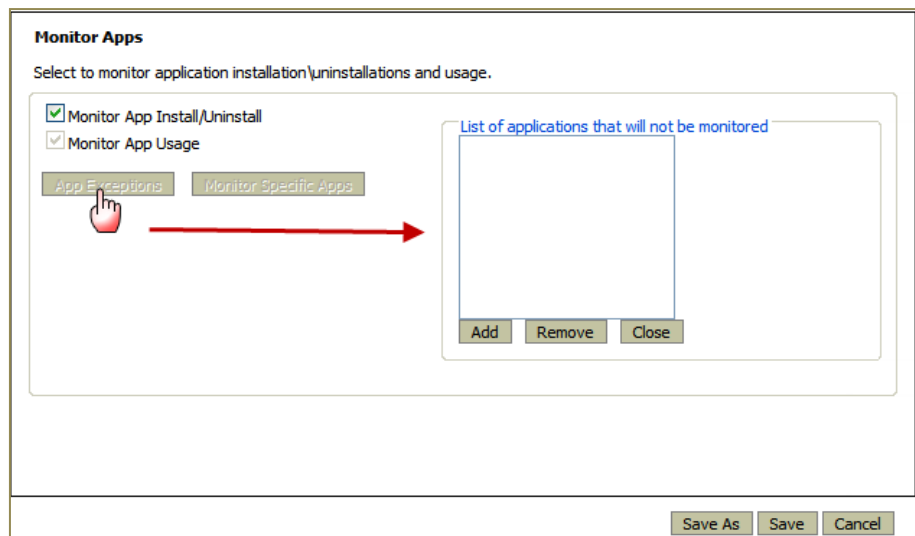
Filtering Applications that need not be monitored

To filter out applications that need not be monitored

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Select the **Monitor App Usage** checkbox, if not selected.
- 4 Click **App Exceptions**.

EventTracker displays 'List of applications that will not be monitored' pane.

Figure 297
App Exceptions

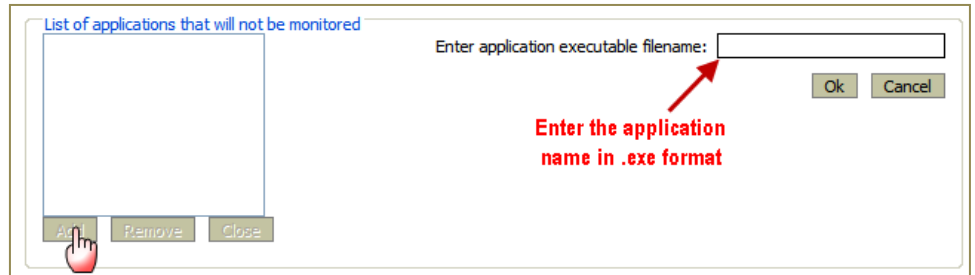


- 5 Click the **Add** button.

EventTracker opens a textbox to type the file name of the applications.

Figure 298
App Exceptions

Application name
should be in .exe
format.



- 6 Type the application name with **.exe** extension that you do not want to monitor.
- 7 Click **OK**.
- 8 Click **Save**.

Filtering Applications that need to be monitored

To monitor specific applications

- 1 Move to the Windows Agent Configuration page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Select the **Monitor App Usage** checkbox, if not selected.
- 4 Click **Monitor Specific Apps**.

EventTracker displays 'List of app executables' pane.

- 5 Click **Add**.

EventTracker opens a textbox to type the file name of the applications.

- 6 Type the application name with **.exe** extension that you want to monitor.
- 7 Click **OK**.
- 8 Click **Save**.

Application name
should be in .exe
format.

Monitoring Services

By default, EventTracker monitors all Windows Services for stop/start. If a service stops, an event will be sent immediately to the Manager. An event will also be sent if a stopped service restarts.

You can also choose to automatically restart services that have been stopped.

There may be certain services that you may not want to monitor. You can filter out such services from the monitoring list.

The service name that needs to be configured can be either the name as displayed in **Control Panel -> Services** or the display name. While configuring the service name, please ensure that it is spelt correctly.

Configuring Service Restart List

This option helps to add services to the restart list.

To configure services that needs to be restarted on stopping

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Services** tab.
EventTracker displays the **Services** tab.

Figure 299
Services tab

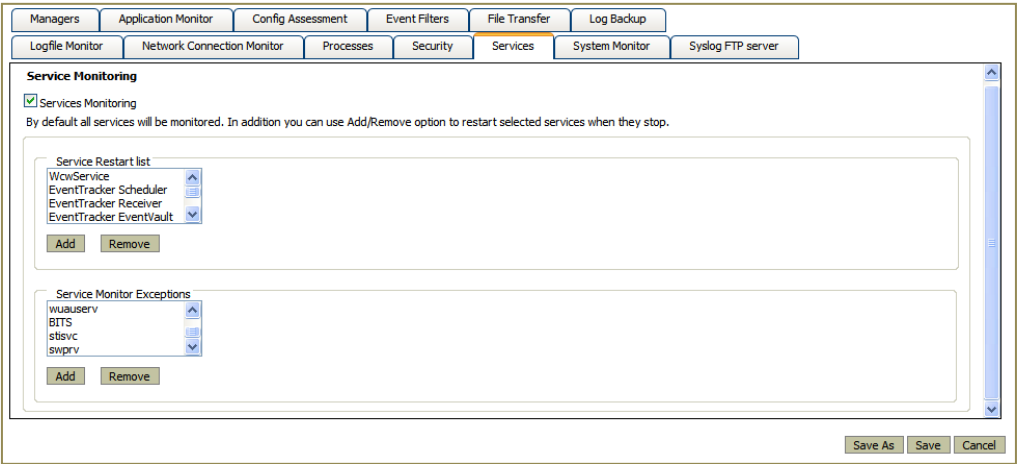


Table 98

Field	Description
Services Monitoring	This checkbox is selected by default to monitor all Windows services. 'Service Restart List' and 'Service Monitor Exceptions' will be enabled only if 'Service Monitoring' checkbox is selected.
Service Restart List	By default following services are monitored: <div> <div>EventTracker Alerter</div> <div>StatusTracker</div> <div>EventTracker EventVault</div> <div>TrapTracker</div> <div>EventTracker Indexer</div> <div>EventTracker Reporter</div> <div>EventTracker Receiver</div> <div>WcwService</div> <div>EventTracker Remoting</div> <div>EventTracker Scheduler</div> </div>

Field	Description
	Click Add to add selected services to restart when they stop. Click the Remove button to remove the services from the 'Services restart list'.
Service Monitor Exceptions	Click Add to add services that you do not want to monitor. Click Remove to remove the services from the list.

- Click **Add** under **Service Restart List**.

EventTracker displays the **Enter Service Name** field to type the name of the service.

Figure 300
Services tab



- Type the name of the service, and then click **OK**.
- Click **Save**.

Filtering Services

To filter out services that need not be monitored

- Move to the 'Windows Agent Configuration' page.
- Select the system from the **Select System** hyperlink.
- Click the **Services** tab.
- Click the **Add** button under **Service Monitor Exceptions**.
- Type the name of the service that you do not wish to monitor in the **Enter Service Name** field.
- Click **OK**.
- Click **Save**.

Monitoring Logfiles

This option enables you to monitor multi-vendor log files with matching keyword entries. EventTracker generates an event if any matching record is found. The Log file monitoring configurations can be done through **EventTracker Agent Configuration** provided on the **EventTracker Control Panel**. In the EventTracker Enterprise (Web GUI), you can only view the Logfile monitoring settings.

To add a log file to monitor

- 1 Double-click **EventTracker Agent Configuration** on the EventTracker Control Panel.
- 2 Select the system from the **Select System** drop-down list.
- 3 Click the **Logfile Monitor** tab.
EventTracker opens the 'Logfile Monitor' tab.

Figure 301
Logfile Monitor tab

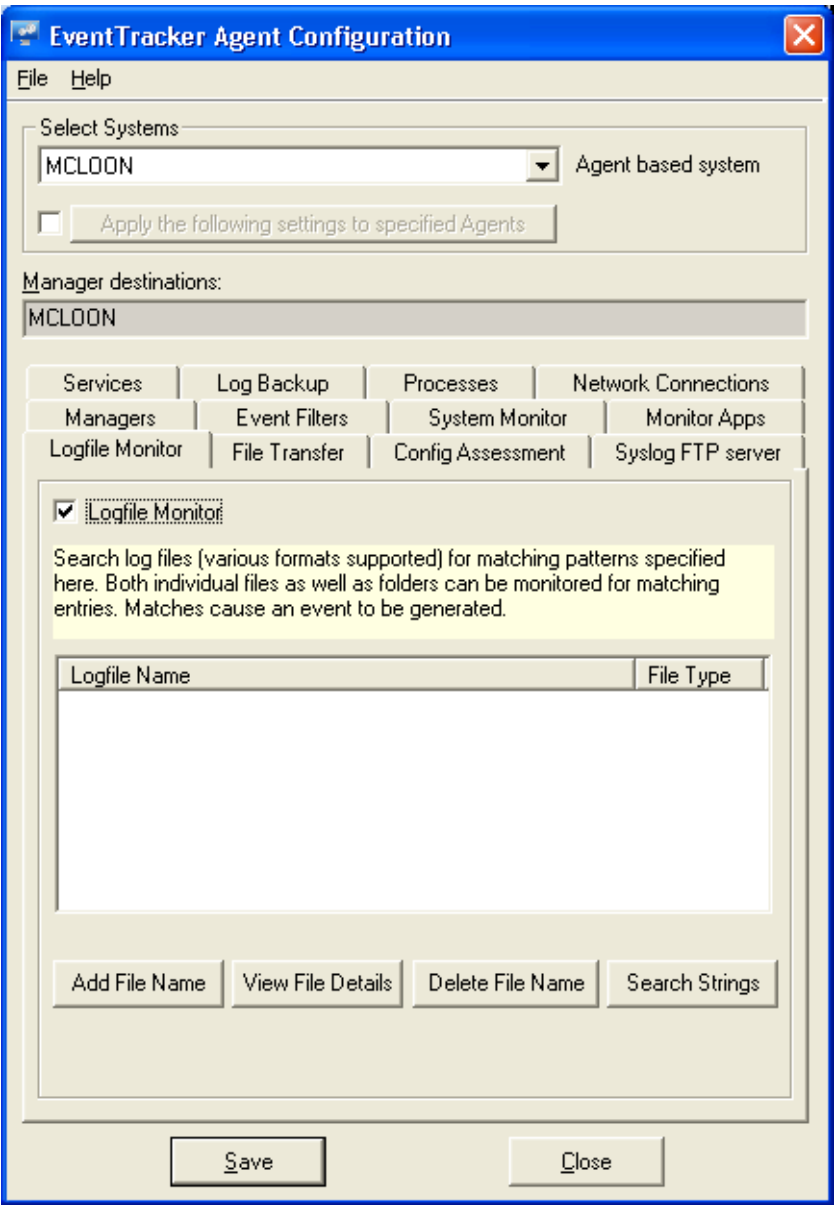
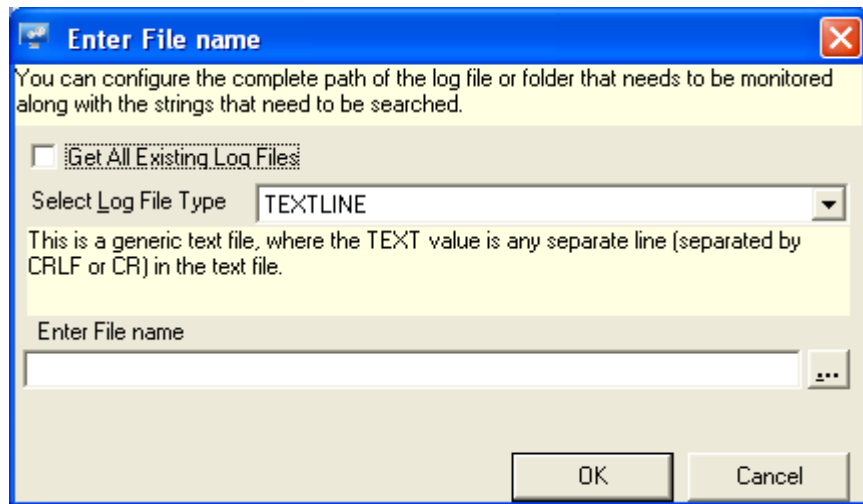


Table 99

Click	To
Add File Name	Add a log file that you wish to monitor.
View File Details	View log file details.
Delete File Name	Delete the log file name from the list.
Search Strings	Configure the strings to search.

- 4 Click the **Add File Name** button.
EventTracker displays the 'Enter File Name' window.

Figure 302
Add file name



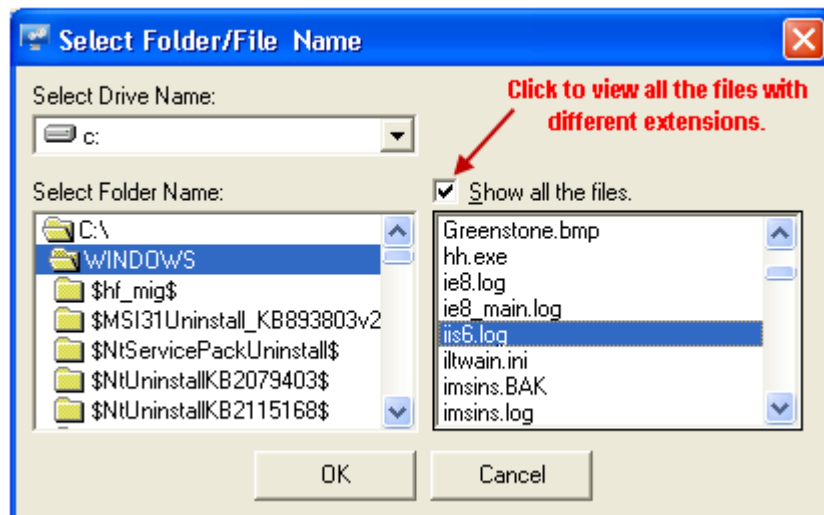
- 5 Click the **Get All Existing Log Files** checkbox, if you want all the existing files prior to this configuration and the files that are logged after this configuration.
- 6 Select the logfile type from the **Select Logfile Type** drop-down list.
- 7 Type the path in the **Enter File Name** field.

(OR)

Click the browse button  to locate the log file.

EventTracker displays the 'Select Folder/File Name' dialog box.

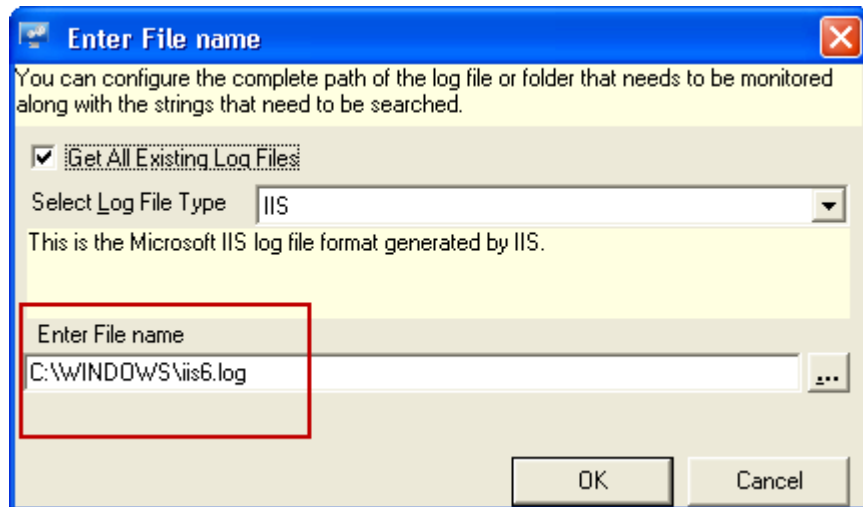
Figure 303
Select Folder/File
Name dialog box



- 8 Select the **Show all the files** checkbox to view all files with different file extensions.
- 9 Go to the appropriate folder, and then select an appropriate file which is associated with the selected 'Log File Type'

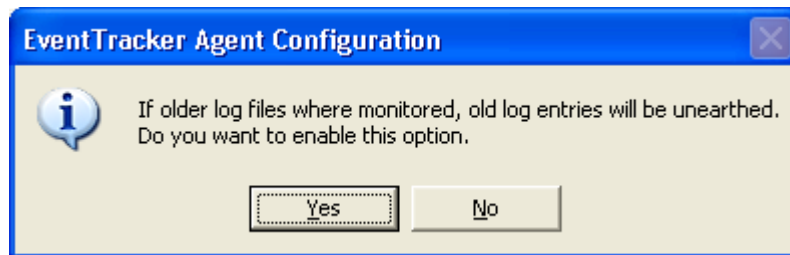
- 10 Click **OK**.
EventTracker displays the 'Enter File Name' window with the file location.

Figure 304
Enter File Name
dialog box



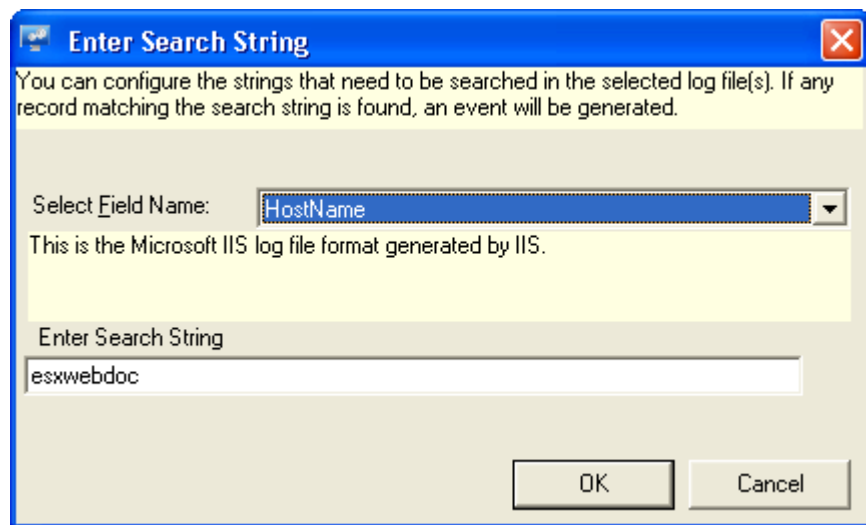
- 11 Click **OK**.
EventTracker displays the 'EventTracker Agent Configuration' message box.

Figure 305
EventTracker Agent
Configuration
message box



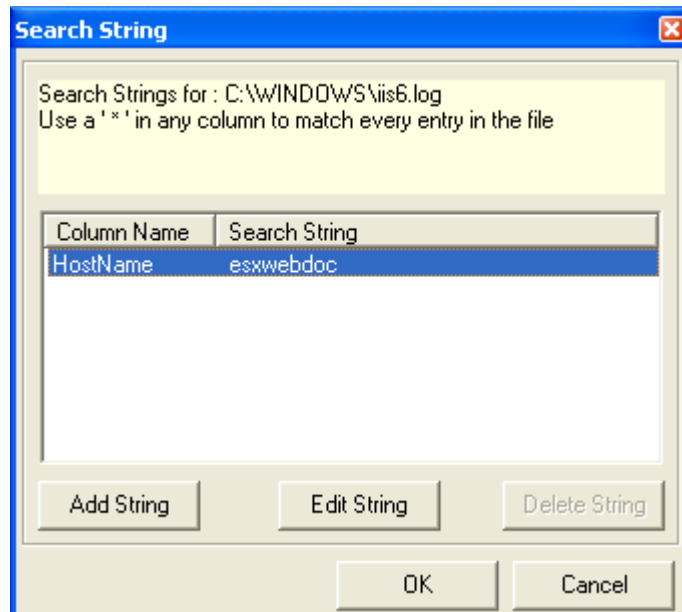
- 12 Click **Yes**.
EventTracker displays the Search String dialog box.
- 13 Click the **Add String** button.
EventTracker displays the 'Enter Search String' dialog box.
- 14 Select the file name from the **Select Field Name** drop-down list. (See figure 332)

Figure 306
Enter Search String
dialog box



- 15 Type the string that you want to search in the **Enter Search String** field.
EventTracker displays the Enter Search String dialog box.
- 16 Click **OK**.
EventTracker displays the Search String dialog box.

Figure 307
Search String
window



- 17 Click **OK**.
EventTracker displays the 'Agent Configuration' window with the newly added Logfile entry.

Figure 308
Agent Configuration
window – Logfile
Monitor tab

Clear the
checkbox against
the newly added
logfile name to
exclude the file
from monitoring.

☒ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type
<input checked="" type="checkbox"/> C:\WINDOWS\iis6.log	IIS


Clear this checkbox to exclude the file from monitoring.

18 Click the **S**ave button.

GOOD TO KNOW:

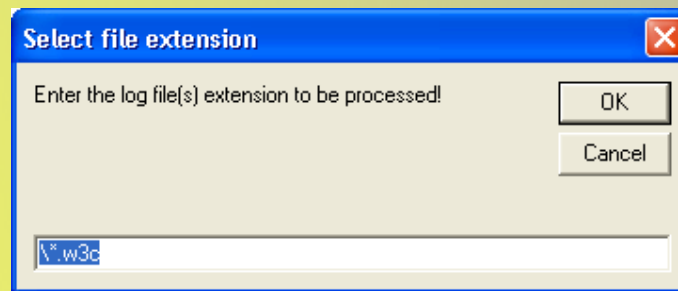
To select multiple files with the same or different file extension:

You can select multiple files with the same or different file extension by using wildcard character *. Click the **Add File Name** button.

In the **Enter File name** window, click the browse button  to locate the log file.

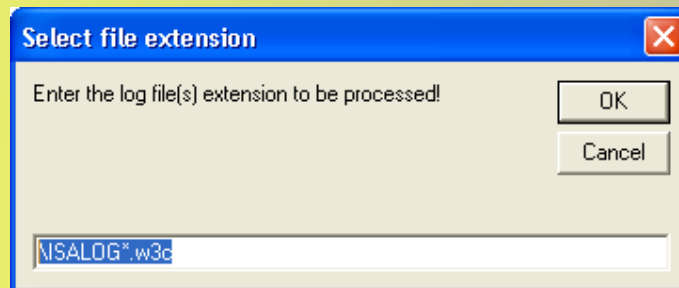
In the **Select Folder/File Name** dialog box, click the **OK** button. (Do not select the file name from the folder.)

EventTracker displays the 'Select File Extension' window.

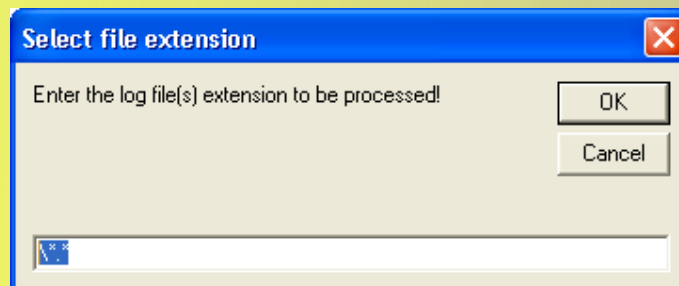


Type the file name in the given field or leave as it is to consider all files in the selected folder with file extension 'w3c' for monitoring.

If you are specifically interested in monitoring ISA Firewall log files, type the file name as "ISALOG*"



To select multiple files irrespective of file extensions, type '*.*'.



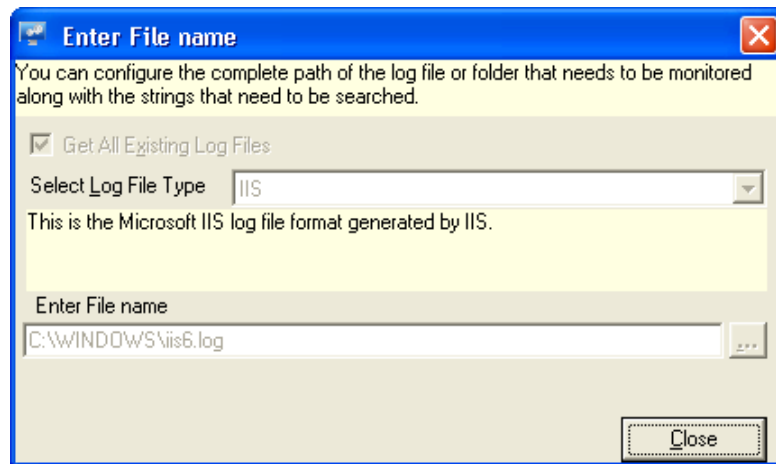
Viewing File Details

This option helps you view files details.

To File Details

- 1 In EventTracker Control panel, open the **EventTracker Agent Configuration** window.
- 2 Select the system from the **Select Systems** drop-down list.
EventTracker displays the 'Logfile Monitor' tab.
- 3 Click the **Logfile Monitor** tab.
- 4 Select the log file from the list under **Logfile Name**.
- 5 Click **View File Details**.
EventTracker displays the 'Enter File Name' window.

Figure 309
Enter File Name
dialog box



- 6 Click **C**lose.

Deleting Log File Monitoring Settings

This option helps you delete log file monitoring settings.

To delete log file monitoring settings

- 1 In EventTracker Control panel, open the **EventTracker Agent Configuration** window.
- 2 Select the system from the **Select Systems** drop-down list.
- 3 Click the **Logfile Monitor** tab.
- 4 Select the log file from the **Logfile Name** list.
- 5 Click **Delete File Name**.
- 6 Click **S**ave on the Agent Configuration window.

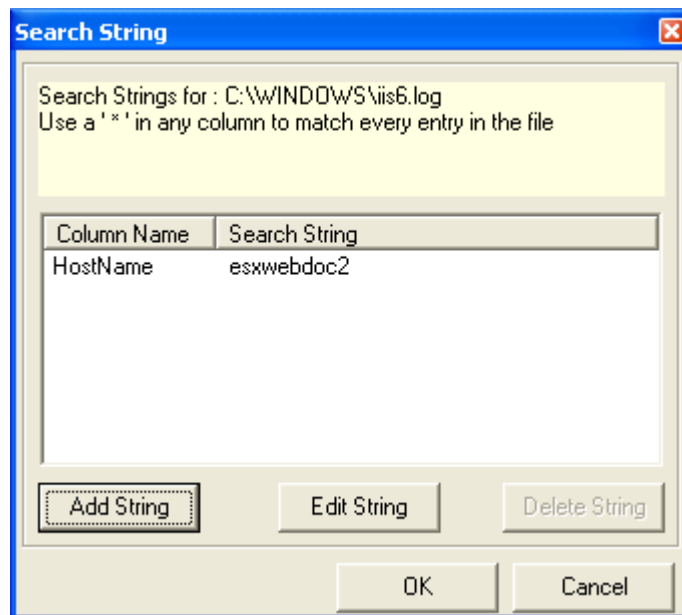
Searching Strings

This option helps you search strings.

To search string

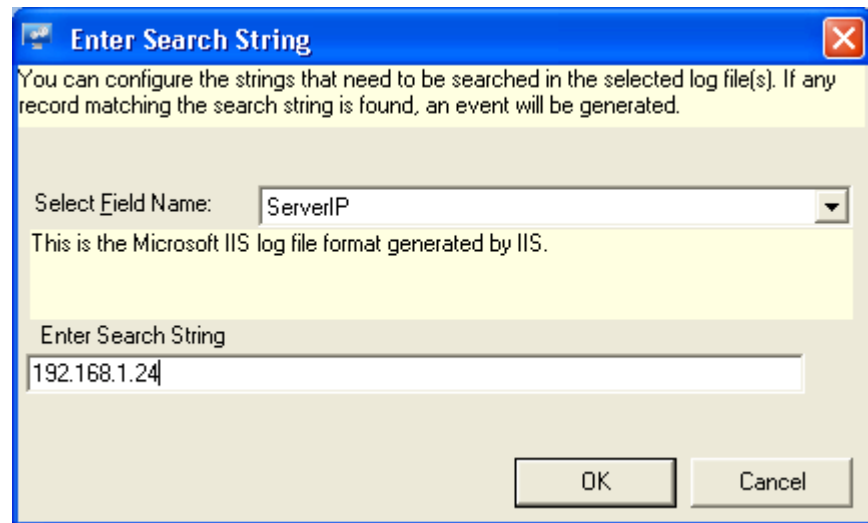
- 1 In EventTracker Control panel, open the **EventTracker Agent Configuration** window.
- 2 Select the system from the **Select Systems** drop-down list.
- 3 Click the **Logfile Monitor** tab.
- 4 Select the log file from the **Logfile Name** list.
- 5 Click **Search Strings**.

Figure 310
Search String
window



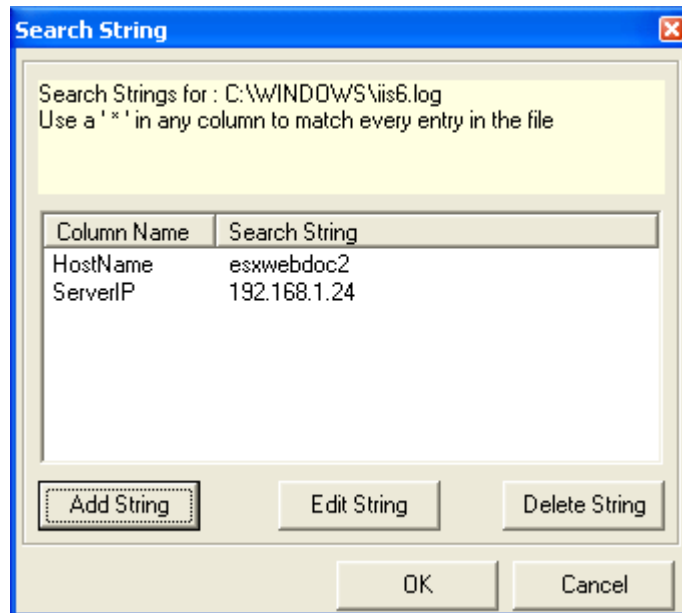
- 6 Click **Add String**.
EventTracker displays the Enter Search String dialog box.
- 7 Select the file name from the **Select Field Name** drop-down list.
- 8 Type the string that you want to search in the **Enter Search String** field.
EventTracker displays the Enter Search String dialog box with newly added search string entry.

Figure 311
Enter Search String
dialog box



- 9 Click **OK**.
EventTracker displays the Search String dialog box with newly added search string.

Figure 312
Search String
window



To modify, click **Edit String**. Enter appropriately in the relevant fields in the displayed **Enter Search String** dialog box, and then click **OK**.

OR

To delete, select the string you want to delete and then click **Delete String** in the **Search String** dialog box.

- 10 Click **OK** on the 'Search String' dialog box.

EventTracker displays the 'Agent Configuration' window with the modified settings.

11 Click **Save**.

Viewing File Details – Web UI

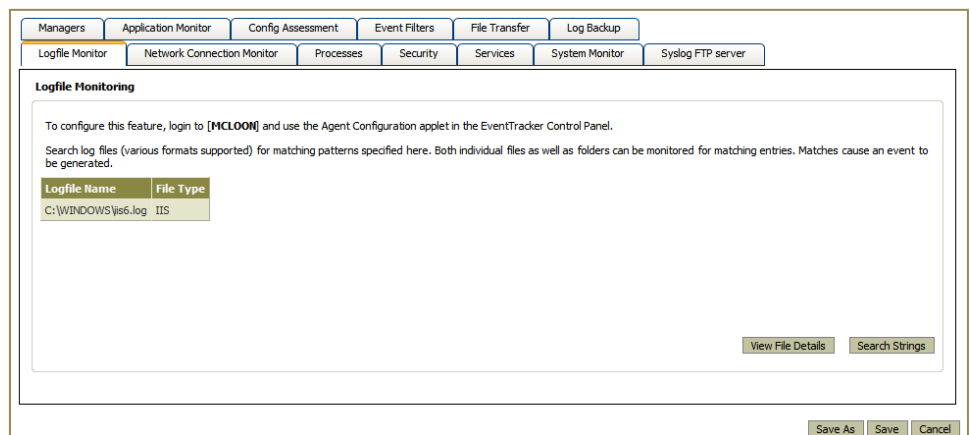
This option helps you view file details through Web UI.

To view file details

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** hyperlink at the upper-right corner.
- 3 Click **Windows Agent Config**.
- 4 Select the system from **Select System** hyperlink.
- 5 Click the **Logfile Monitor** tab.

EventTracker displays the Logfile Monitoring page with configuration settings you have set earlier.

Figure 313
Logfile monitoring



- 6 Select a row, and then click **View File Details** button

EventTracker displays the View Details pop-up window.

Figure 314
Logfile Monitoring –
View Details



- 7 Click the **Ok** button to close the window.

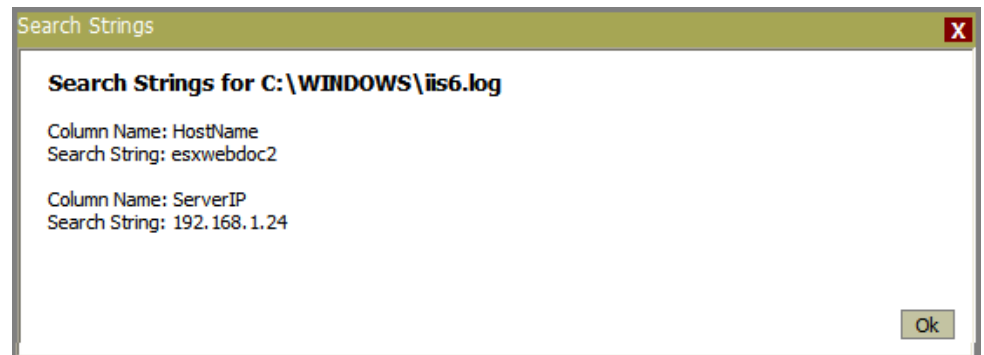
Viewing Search Strings – Web UI

This option helps you view search strings through Web UI.

To search strings

- Select a row and then click **Search Strings**.
EventTracker displays the Search Strings pop-up window.

Figure 315
Logfile Monitoring –
Search Strings



Click the **Ok** button to close the window.

Monitoring Check Point Logs

This option helps you monitor logs generated by Check Point.

To monitor Check Point logs

- 1 In EventTracker Control panel, open the **EventTracker Agent Configuration** window.
- 2 Select the system from the **Select System** drop-down list.
- 3 Click the **Logfile Monitor** tab.
- 4 Click the **Add File Name** button.
EventTracker displays the Enter File Name dialog box.
- 5 Select the logfile type as 'CHECKPOINT' from the **Select Logfile Type** drop-down list.

EventTracker unfolds a pane with configuration options.

Figure 316
Enter File Name
dialog box

- 6 Select an option from the **Communication Method** drop-down list.

Table 100

Communication method options	Description
OPSEC_SSLCA	Encryption Method: 3DES Compressed: No
OPSEC_SSLCA_COMP	Encryption Method: 3DES Compressed: Yes


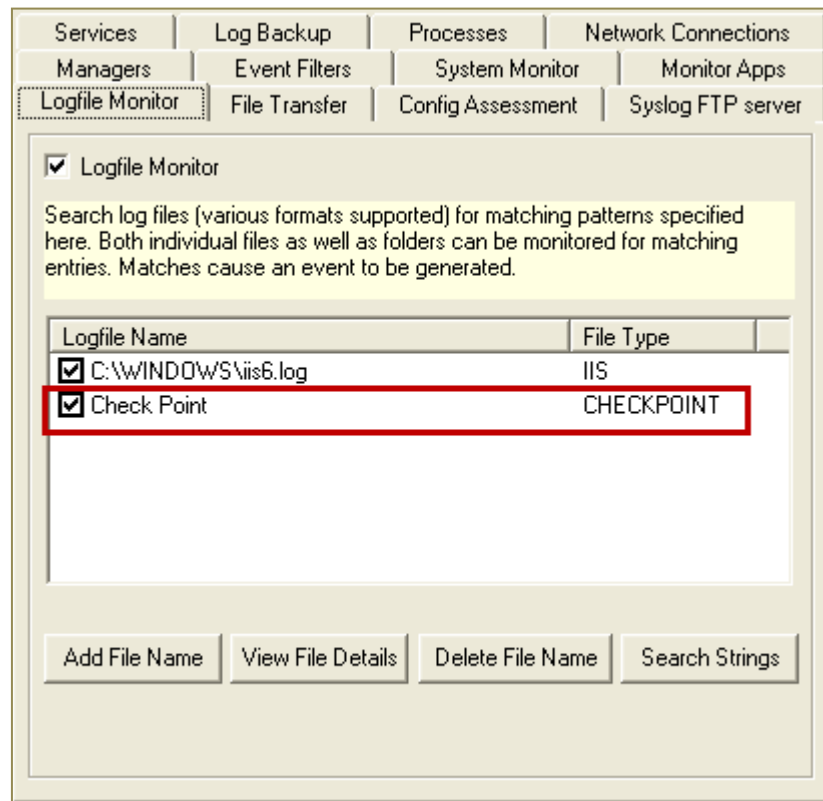
- 7 Type **LEA Server Name**.
- 8 Type the **Client DN**.
Check Point generated this string while configuring the OPSEC Application.
- 9 Type the **Server DN**.
This is the Check Point Gateway DN.
- 10 Click the browse button  to locate SSLCA file.
- 11 Select the SSLCA file and then click **Open**.
EventTracker populates the SSLCA file field
- 12 Type the **Server IP**.
This is the IP of the host where Check Point is installed.
- 13 Type the **Server Port**.
This can any port but should be consistent with what you have entered earlier in the fwopsec.conf file.

Table 101

Field	Description
Active	This option is selected by default. Select this option to receive live Check Point logs from the point in time the configuration takes effect.
Historical	Select this option to read from previous logs and the current logs as well. This option has two modes namely Current Logs and All Logs . Select the Current Logs option to read from the first record of the current log. This mode is selected by default. Select the All Logs option to read from all the backed up logs and the current logs.

- 14 Click **OK**.
EventTracker displays the 'Agent Configuration' window.

Figure 317
ETA- Logfile Monitor
tab



15 Click **Save**.

Monitoring VMware Logs

This option helps you monitor logs generated by VMware.

To monitor VMware logs

- 1 In EventTracker Control panel, open the **EventTracker Agent Configuration** window.
- 2 Select the system from the **Select System** drop-down list.
- 3 Click the **Logfile Monitor** tab.
- 4 Click the **Add File Name** button.
EventTracker displays the 'Enter File Name' dialog box.
- 5 Select the logfile type as VMWARE from the **Select Logfile Type** drop-down list.
EventTracker unfolds a pane with configuration options.

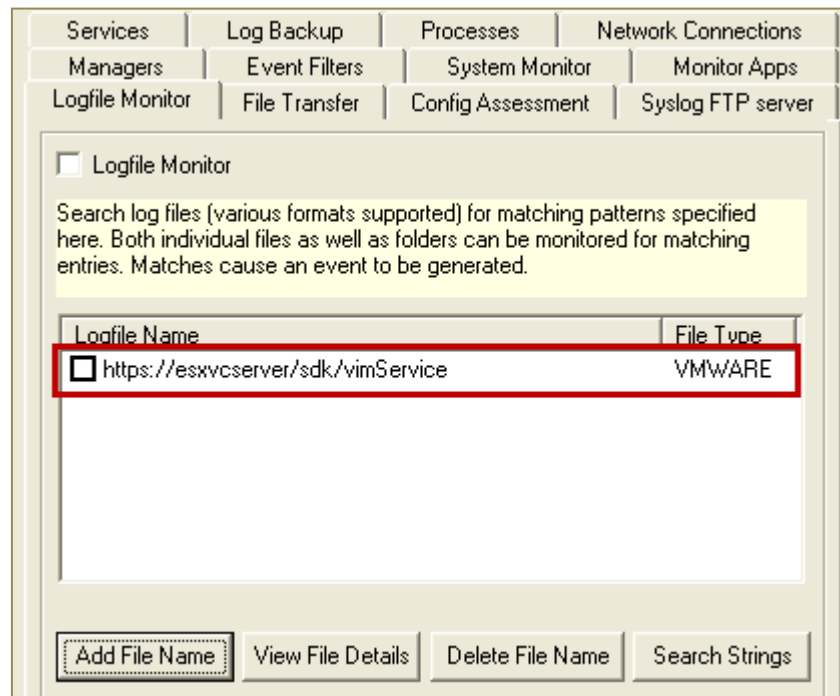
Figure 318
Enter File Name
dialog box

Table 102

Field	Description
VMware URL	Type a valid URL, e.g. https://esxvcserver/sdk/vimService You can also replace the server name with the IP address.
User Name	Type valid user name.
Password	Type valid password.
Timeout	Time connection timeout.

- 6 Type appropriately in the relevant fields.
 - 7 Click **Test Connection** to check if the configuration parameters you have entered are correct.
 - 8 Click **OK**.
- EventTracker displays the Agent Configuration window.

Figure 319
EventTracker Agent
Configuration
window



9 Click **Save**.

Monitoring Network Connections

NCM (Network connection monitoring) provides you with the capability to effectively monitor for network connections on any system in your enterprise. It is a feature that provides you security beyond the firewall by detecting threats from inside the firewall as well as keeping the external attackers at bay.

It helps you keep track of various happenings like connections established by remote applications, unauthorized connections to server and connections made to standard ports.

NCM provides second level security beyond firewall. NCM can drastically reduce internal security threats and can be configured to raise an alert whenever any intruder outside a list of trusted IP addresses attempts to make network connection. The NCM functionality can also be set at high security mode wherein an event is generated for all incoming and outgoing connections.

The NCM functionality facilitates to achieve the following key objectives:

- Host based intrusion detection
- To provide second level security and complement to firewall and anti-virus
- In strengthening security policies
- To improve security policies against inside security breaches

- To monitor all network connections (TCP and UDP)
- For constant unattended, reliable monitoring of intrusion detection
- Flexible configuration as per the business requirement

To monitor network connections

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Network Connection Monitor** tab.

EventTracker displays the 'Network Connection Monitor' tab.

Figure 320
Network Connection
Monitor tab

Table 103

Field	Description
TCP	This checkbox is selected by default to monitor TCP network connections.
UDP	This checkbox is selected by default to monitor UDP network connections.
Connection States	
Open	This checkbox is selected by default to monitor opened TCP/UDP connections.
Changed	Select this checkbox to monitor TCP/UDP connections whose connection state has been changed recently.
Close	This checkbox is selected by default to monitor closed TCP/UDP connections.
All Network Traffic (NCM): By default, EventTracker selects this option.	
Exclude List	Click this button to configure the network connections that need not be monitored. A notification will be sent for the entries in this list, if the port is open.

'Network connection monitoring' page will display the default selections only if the 'Network connection monitoring' checkbox is selected while installing EventTracker Enterprise.

If a port is present in both the 'Include list' as well as 'Exclude list', then that port will be monitored and no notifications will be sent for the same, though it can be seen in both the lists.

Field	Description
Include List	Click this button to configure the network connections to monitor. Entries in this list will always be monitored. 'Include Network Connections List' always override the 'Exclude Network Connections List'.
Suspicious Traffic Only (SNAM)	
Trusted List	Click this button to view and configure trusted network connections.

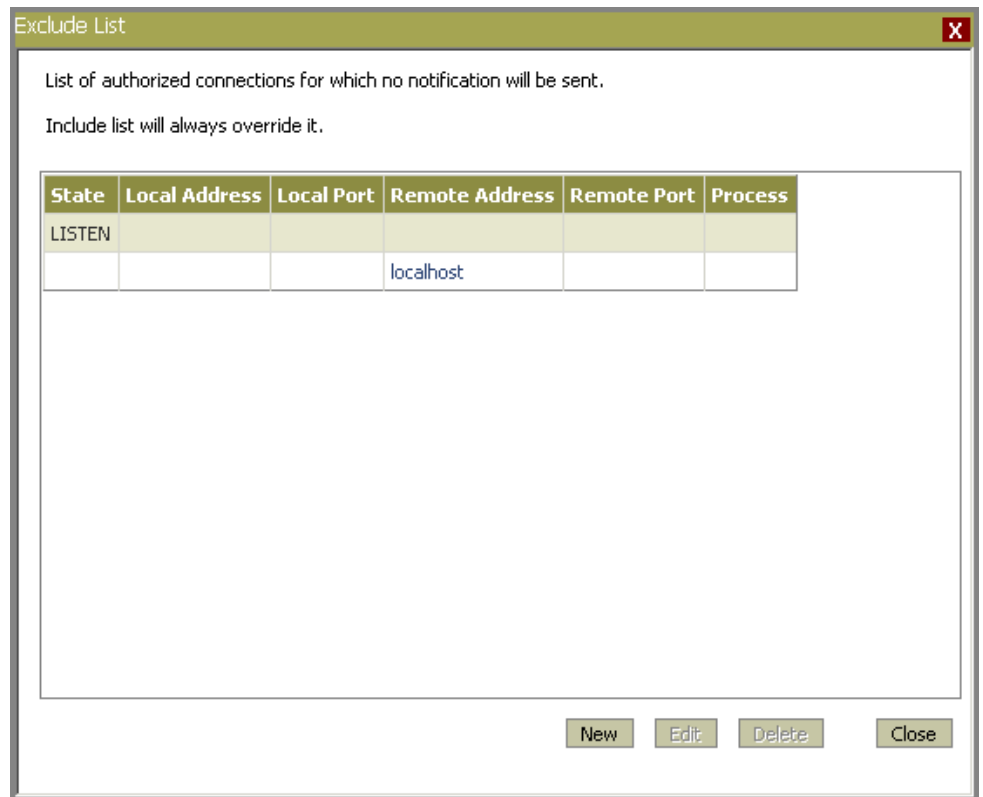
- 4 Select or clear the **TCP** or **UDP** checkbox.
- 5 Click the **Save** button.

Excluding Network Connections

To configure network connections that need not be monitored

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Network Connection Monitor** tab.
- 4 Click **Exclude List**.
EventTracker displays the Exclude List pop-up window.

Figure 321
Exclude List window



- 5 Click **New**.

EventTracker displays the Exclude List window to type Network Connection Details.

Figure 322
Network Connection
Details window

Exclude List

Local Address Details

Host Name or IP Address:

Local Port:

Remote Address Details

Host Name, IP Address or URL:

Remote Port:

Select IP Address Range

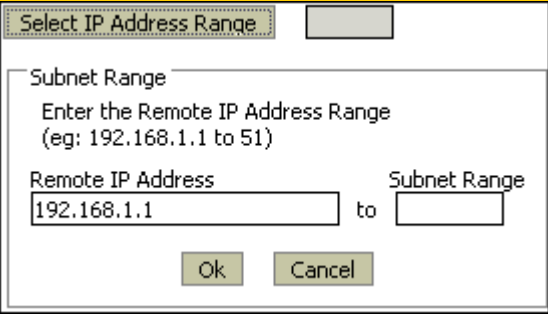
Process Name: (e.g. iexplore.exe)

Connection State:

Ok Cancel

Table 104

Field	Description
Local Address Details	
Host Name or IP Address	Type the host name or the IP address in this field.
Local Port	Select a local port from the drop-down list.
Remote Address Details	
Host name, IP Address or URL	Type the host name, IP address or URL in this field.
Remote Port	Select a remote port from the drop-down list.
Select IP Address Range	Click this button to add IP address range. EventTracker displays the IP Address Range Setting dialog box.

Field	Description
	 <p>Type the range until which you want to monitor the IP network connections.</p> <p>This option is available only when you Type the IP address in the Host name, IP address or URL field.</p>
Process Name	Type the process name in this field.
Connection State	Select a connection state from the drop-down list.

 Note

If a field is left blank, a wildcard match for that field is assumed. For example, leaving the Local Port field blank implies that any value in that field is acceptable.

6 Type appropriately in the relevant fields.

Figure 323
Network Connection
Details window

Exclude List

Local Address Details

Host Name or IP Address: esxwebdoc

Local Port: 25

Remote Address Details

Host Name, IP Address or URL: obelix

Remote Port: 110

Select IP Address Range

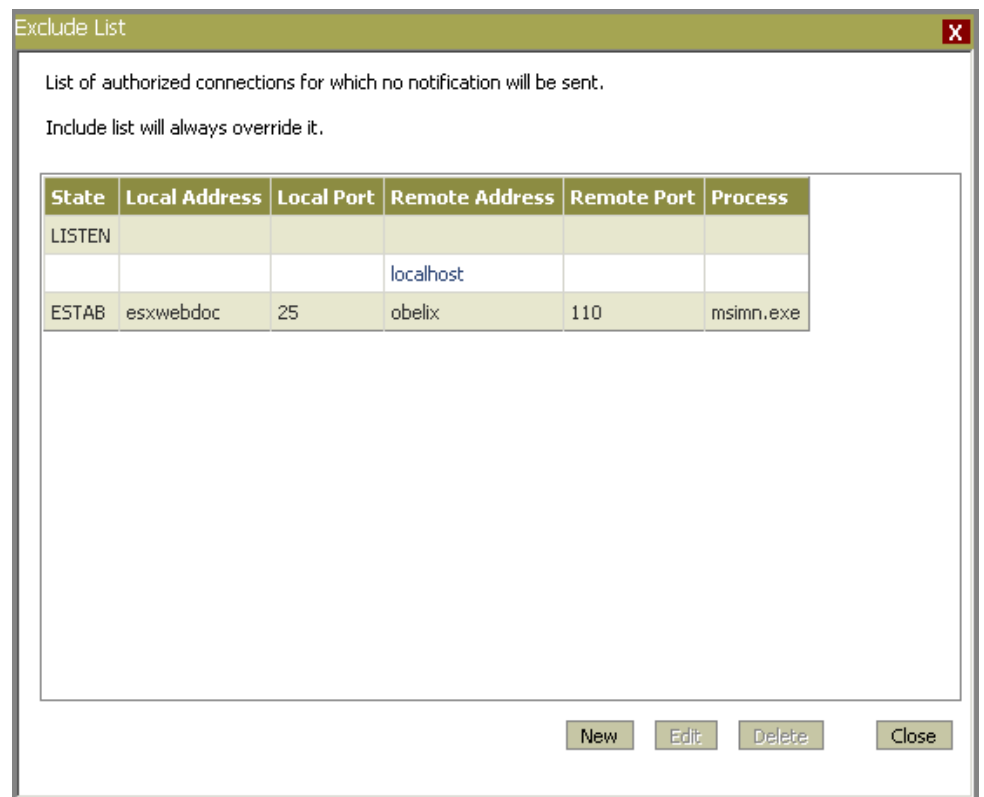
Process Name: (e.g. iexplore.exe) msimn.exe

Connection State: ESTAB

Ok Cancel

- 7 Click **OK**.
EventTracker displays the Exclude List with the newly added entry.

Figure 324
Exclude List window



- 8 To modify the network connection details, click **Edit**.
- 9 To delete the network connection details, select the network connection details you want to delete from the list, and then click **Delete**.
- 10 Click **Close** on the Exclude List pop-up window.
- 11 Click **Save**.

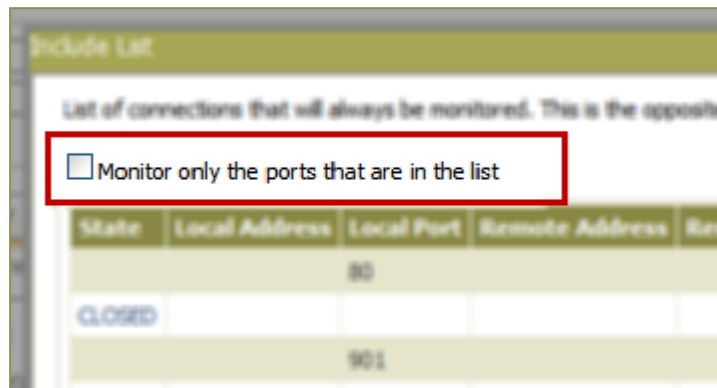
Including Network Connections for Monitoring

To configure network connections to monitor

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Network Connection Monitor** tab.
- 4 Select the appropriate checkboxes.
- 5 Click **Include List**.

EventTracker displays the Include List pop-up window.

- 6 Select the **Monitor only the ports that are in this list** checkbox to monitor only the ports present in the list, and then click **Close**.



- 7 To add more network connection details, click **New**.
EventTracker displays the Include List window to type network connection details.
- 8 Type appropriately in the relevant fields.

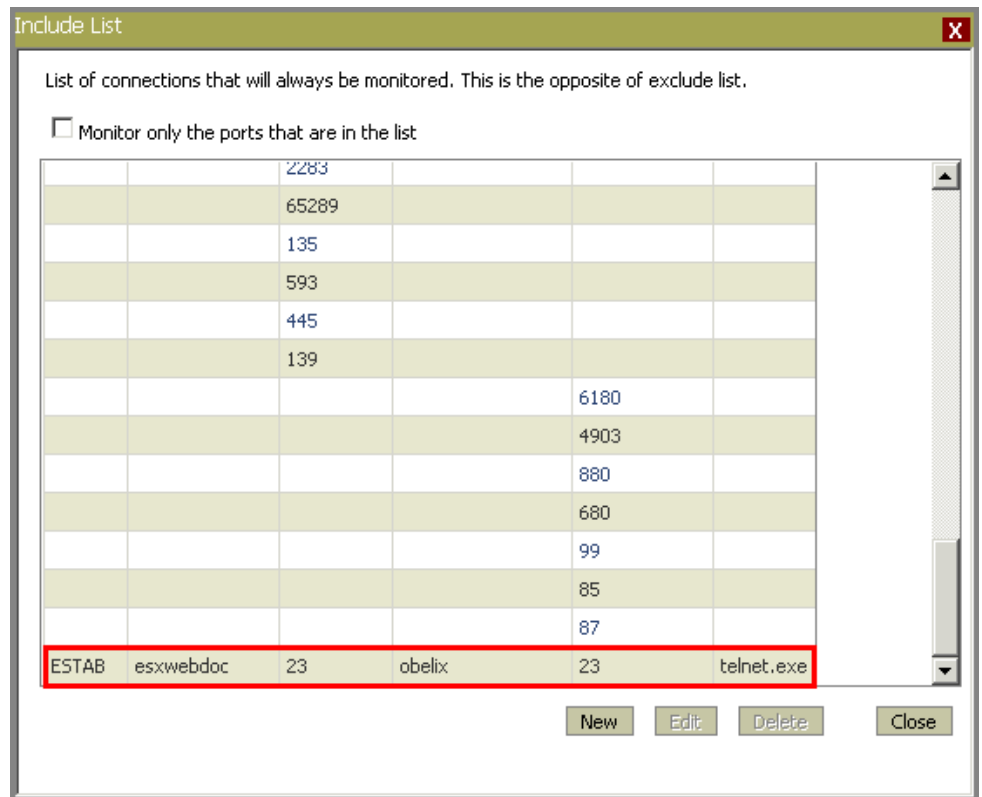
Figure 325
Network Connection
Details window

The screenshot shows the 'Include List' window with the following fields and options:

- Local Address Details:**
 - Host Name or IP Address:
 - Local Port:
- Remote Address Details:**
 - Host Name, IP Address or URL:
 - Remote Port:
 -
- Process Name:** (e.g. iexplore.exe)
- Connection State:**
-

- 9 Click **OK**.
EventTracker displays the Include List with the newly added entry.

Figure 326
Include List window



- 10 To modify the network connection details, click **Edit**.
- 11 To delete the network connection details, select the network connection details you want to delete from the list, and then click **Delete**.
- 12 Click **Close**.
- 13 Click **Save**.

Suspicious Connections

This feature is an enhancement of the existing 'Network Connection Monitoring'. This option enables you to monitor the suspicious usage of TCP or UDP ports and their connection states. By default, all the connections are suspicious and you can exempt applications and ports from monitoring. EventTracker is shipped along with a list of applications and ports, which are not harmful to any enterprise environment. As discussed, EventTracker Agent will not monitor these White-listed applications and ports.

 Note

Prior to enabling EventTracker Agent to monitor Suspicious Traffic, apply all the latest Microsoft patches / hotfixes if the operating system is Windows 2000.

Monitoring Suspicious Connections

This option helps you to monitor suspicious connections and to view predefined trusted connections list. EventTracker does not monitor the connections listed in Trusted List. You can also edit predefined trusted connection list and define your own set of trusted connection list.

To view Trusted List

- 1 In EventTracker Control panel, open the **EventTracker Agent Configuration** window.
- 2 Select the system from the **Select Systems** drop-down list.
- 3 Click the **Network Connection Monitor** tab.
EventTracker displays the Network Connection Monitor tab.
- 4 Select the **Suspicious Traffic Only (SNAM)** option.
- 5 Click the **Trusted List** button.

EventTracker displays the 'Trusted Connections List' dialog box.

EventTracker exempts enabled connections listed in the **Trusted List** from monitoring.

Figure 327
Trusted
Connections List

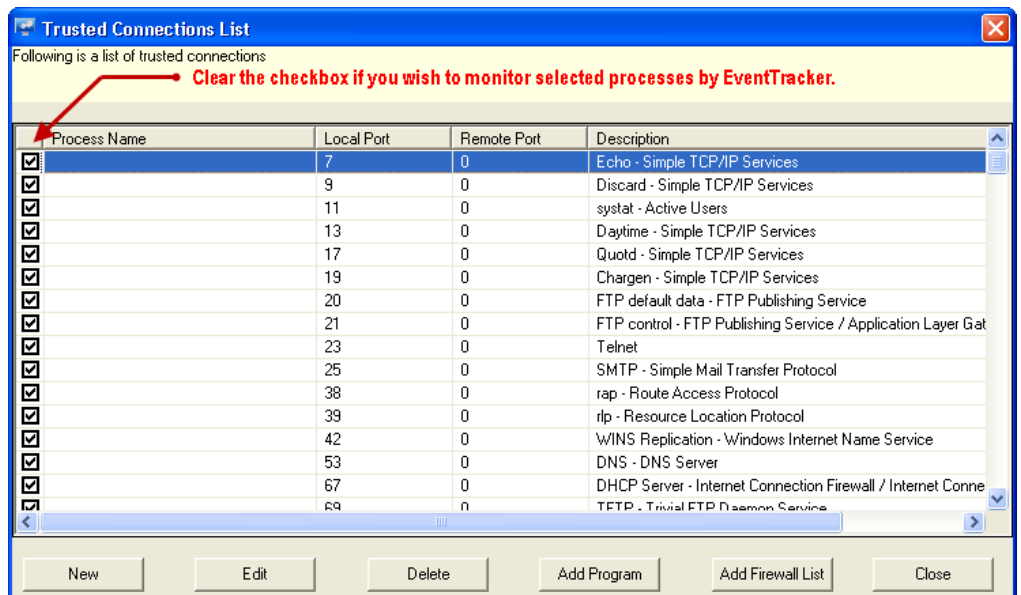

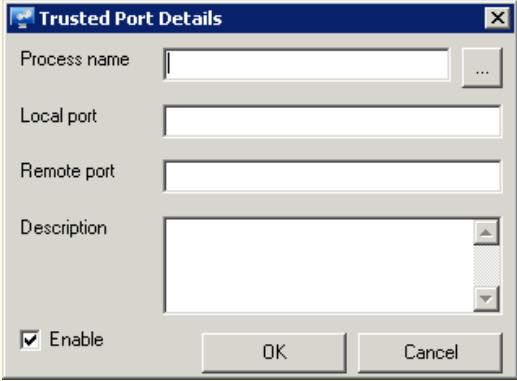

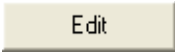

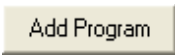

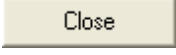


Table 105

Click	To
	<p>Add new trusted connections. EventTracker displays 'Trusted Port Details' dialog box.</p>  <p>Type appropriate details in the relevant fields and then click OK. You can use wild cards to search processes. For example, had you configured Virtual Collection Points and wish to add all EventTracker Receiver processes, it is enough to provide the Process name as EtReceiver*.exe.</p> <p>You can also use  browse button to locate the process.</p>
	<p>Select a process from the list and then click Edit. EventTracker displays 'Trusted Port Details' dialog box. Edit required details in the relevant fields and then click OK.</p>
	<p>Select a process from the list, and then click Delete. EventTracker displays confirmation message box. Click Yes to delete the selected entry.</p>
	<p>Add programs installed in your computer to the trusted list.</p>
	<p>Add programs included in the Firewall Exceptions list to the trusted list.</p>
	<p>Close the 'Trusted Connections List' dialog box.</p>

GOOD TO KNOW:

Suspicious Traffic Only (SNAM) option helps you to view, enable, and disable predefined trusted connections list.

The connections listed in the **Trusted List** are exempted from monitoring.

The trusted list contains a list of known good applications and ports through which the usual network connections between the processes happen.

You can edit the predefined trusted connection list and can define your own set of trusted connection list.

By default, the **predefined trusted connections are enabled**, which means EventTracker exempts those processes and ports from monitoring.

Clear the checkbox next to the process that you wish to monitor by EventTracker. (See figure 345)

In some rows in the list, you might notice 'Process Name' field is empty, this signifies that any process that communicate through the defined ports are deemed to be legitimate. (See figure 346)

Similarly, in some rows you might notice that the 'Local port' and/or 'Remote Port' are 0 (zero). This signifies that the processes listed could use any available ports to communicate. EventTracker considers that traffic to be legitimate and exempts from

Figure 328
Trusted Connections
List

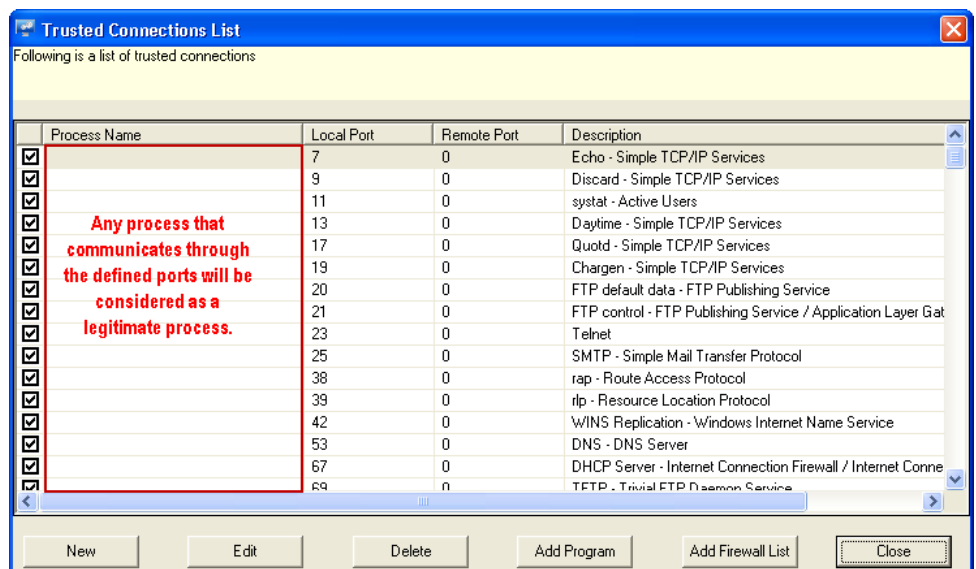
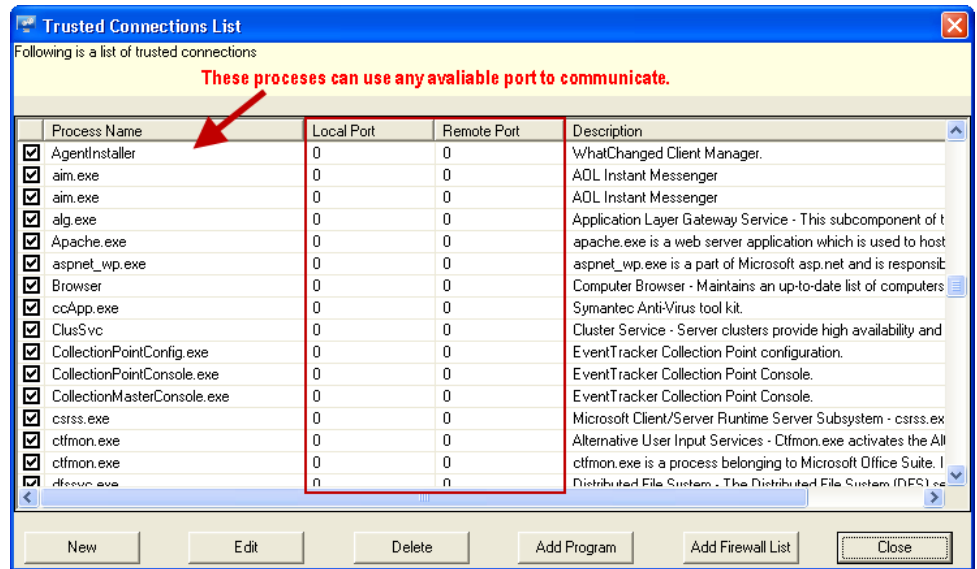


Figure 329
Trusted Connections
List



Adding Programs to the Trusted List

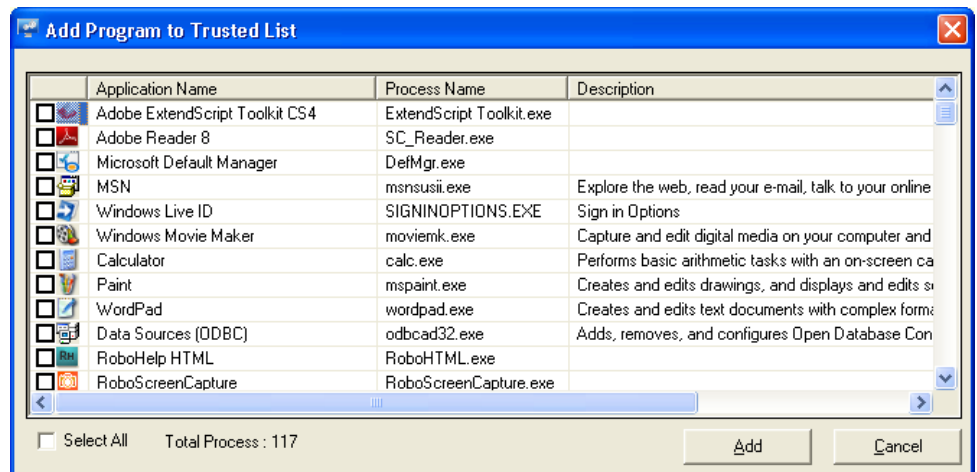
This option helps you add programs installed in your computer to the trusted list. You can enable or disable the entries in the trusted programs list. Enable means the processes and the ports used by the processes are legitimate and disable means illegitimate and EventTracker monitors them.

To add programs to the trusted list

- 1 Click **Add Program**.

EventTracker displays the 'Add Program to Trusted List' window.

Figure 330
Add Program to
Trusted List window



- 2 Select the checkbox against the programs or select the **Select All** checkbox to select all the programs.
- 3 Click **Add**.
EventTracker adds the selected program to the Trusted Connections List.
- 4 Click **Close**.
- 5 Click **Save**.

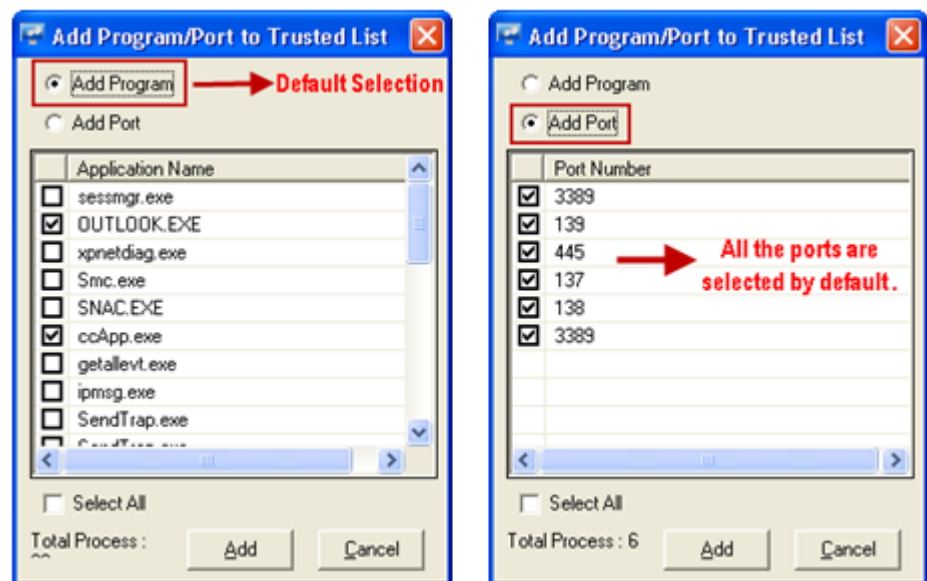
Adding Firewall Exceptions to the Trusted List

This option helps you add the processes and ports in the Firewall programs and ports Exceptions to the trusted list.

To add Firewall Exceptions to the Trusted List

- 1 Click **Add Firewall List**.
EventTracker displays the 'Add Program/Port to Trusted List' window.

Figure 331
Add Program/Port
Trusted List window



By default, EventTracker selects the **Add Program** option and displays the programs in the exceptions list.

Or

Select the **Add Port** option, EventTracker displays available ports in the exception list.

- 2 Select the programs or select the **Select All** checkbox and then click **Add** to add programs to the trusted list.
EventTracker adds the selected items to the 'Trusted Connections' List.

Monitoring Processes

Process monitoring enables the administrator to monitor the general health of processes on a system. You can configure general process health thresholds for CPU and Memory Usage per process. CPU usage is measured in terms of percentage while memory usage is measured in absolute terms.

When the configured threshold is crossed, an event will be generated and reported to the Manager. An event will also be generated when the thresholds are back to below configured levels.

Care is taken not to report spikes in CPU or memory usage by a process. Therefore, when an event is seen that a process is crossing thresholds, you can be sure that this is for a long enough period and need to investigate.

By default, all processes will be monitored and the default threshold limits are 1024MB of Memory Usage and 85% of CPU.

You can also choose to filter out processes that you do not want to monitor. By default, all processes will be monitored.

To configure the process to monitor

- 1 Log on to **EventTracker Enterprise**.
- 2 Click **Admin** dropdown, and then click the 'Windows Agent Config'.
- 3 Select the system from the **Select System** hyperlink.
- 4 Click the **Processes** tab.

EventTracker displays the 'Processes Monitoring' page.

Table 106

Field	Description
<div> <input checked="" type="checkbox"/> CPU Performance (%): <input type="text" value="85"/> <input checked="" type="checkbox"/> Memory Usage (MB): <input type="text" value="1024"/> </div>	
CPU Performance (%)	Select CPU Performance threshold limit from the drop-down list.
Memory Usage (MB)	Type the memory usage threshold limit in MB in this field.

- 5 Click the **Add** button.
EventTracker unfolds an option to type the process name.

Figure 332
Processes tab

Enter Process Name:

Ok
Cancel

- 6 Type the process name in the **Enter Process Name** field.

- 7 Click **OK**.
EventTracker adds the process to the **List of Filtered Processes** pane
- 8 Click the **Save** button.

 **Note**

EventTracker generates the process event when the set threshold value crosses the limit for more than 3 minutes.

Removing Processes from 'List of Filtered Processes'

To remove processes from List of Filtered Processes

- 1 Move to the 'Windows Agent Configuration' page.
 - 2 Select the system from the **Select System** hyperlink.
 - 3 Click the **Processes** tab.
 - 4 Select the process from **List of Filtered processes** pane, and then click the **Remove** button
 - 5 Click the **Save** button.
-

Maintaining Log Backup

This option enables you to backup event logs automatically in the EventTracker Agent directory whenever the event logs are full. EventTracker automatically performs event log backup or archival in the standard Windows event log format (.evt / .evtx format).

To backup event logs automatically

- 1 Move to the 'Windows Agent Configuration' page.
- 2 Select the system from the **Select System** hyperlink.
- 3 Click the **Log Backup** tab.

EventTracker displays Log Backup page.

Figure 333
Log Backup tab

Table 107

Windows Event Log's options can be found in Event Viewer >> Right Click **Log type** >> Click **Properties** >> See the **Log size** pane.

Field	Description
Clear logs as needed	<p>If selected, EventTracker Agent clears log file if and only if offset error is encountered.</p> <p>After clearing, Agent inserts '3241" event to notify the user.</p> <p>In this case, no backup is taken.</p> <p>This is true for any setting of the Windows Event Log's 'When maximum log size is reached" option (i.e. Overwrite events as needed, Overwrite events older than N days, Do not overwrite events (clear log manually))</p> <p>EventTracker log backup and clear operation:</p> <p>Computer: EXCHTEST</p> <p>Log file name: Application</p> <p>Log file backup: Not applicable</p> <p>Log file clear: Success</p> <p>Reason: Received invalid offset error while reading the event log.</p> <p>For more information see Microsoft KB Article #177199.</p>
Backup event logs	<p>If the 'Backup event logs" option is selected, and If the offset is lost at any point, no matter whether 'Clear log after backup" checkbox is selected or not the respective log file will be backed up and cleared and the following 3241 event will be logged.</p> <p>EventTracker log backup and clear operation:</p> <p>Computer: EXCHTEST</p> <p>Log file name: Security</p> <p>Log file backup: C:\Program Files\Prism Microsystems\EventTracker\Agent\ EXCHTEST\ Eventlog_Backup_Security1221683647.evt</p> <p>Log file clear: Success</p> <p>Reason: Invalid offset error while reading the event log.</p> <p>For more information see Microsoft KB Article #177199.</p>
Backup Path	<p>By default backed up log files are stored in the EventTracker installation folder typically, ... \Program Files\Prism Microsystems\EventTracker\Agent</p>
Keep backup files for	<p>If selected, backup files older than selected number of days will be automatically deleted by the agent.</p>

- 4 Select the options appropriately.
- 5 Click **Save**.

Transferring Log Files

This option enables you to transfer Windows and other application log files at scheduled times to the manager. Windows logs that are filtered out by the real time settings are cached for transfer (further filtering is available). This minimizes the EventTracker Receiver service workload and conserves the network bandwidth.

To transfer Windows and application log files

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the Admin dropdown and click **Windows Agent Config**.
- 3 Select the system from **Select System** hyperlink.
- 4 Click the **File Transfer** tab.

Figure 334
File Transfer tab

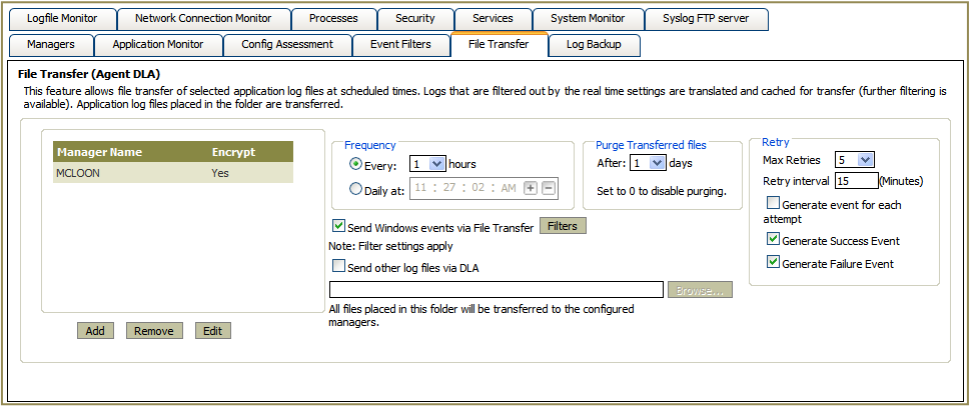


Table 108

Go through the links provided in the [Encryption](#) section to know more about FIPS compliance.

Click button	To
Add	<div>Enter EventTracker Manager name or IP address as destination.</div> <div><div>Add Manager</div><div>Manager: <input type="text"/> Resolve</div><div>Encrypt: No</div><div>OK Cancel</div></div> <div>Type the IP address or name of the Manager in the Manager field.</div> <div>Click the Resolve button to identify newly added manager name or IP</div>

Click button	To
	address and to check its availability in the network. Select an option from the Encrypt drop-down list to encrypt and securely transfer the cached events to the destination. Click OK .
Edit	You can edit the manager name or IP address and even can change the encryption option.
Remove	Delete the destination, i.e. manager name or IP address.

Table 109

Field	Description
Frequency	Set the frequency of file transfer. You can set file transfer to occur every configure hours or daily at a particular time.
Purge Transferred Files	Set this option to purge files that are transferred to the Manager.
Retry	Set the number of attempts made in a given time interval by the source Agent machine to transfer the files to the manager system. You can also generate an event for each transfer attempt, successful transfer or failed transfer as per your choice.
Send Windows Events via File Transfer	Select this option to transfer Windows events to the configured managers at scheduled interval. Click the Filters button to further filter the events. In DLA Filters dialog box, click Add to add the event details.
Send other log files via DLA	Select this option to transfer other application log files. Type the path the folder where log files are dumped or click the browse button to select the folder.
Send Now	Click this option to override the Frequency option and transfer the files immediately. This option is available only under EventTracker Control panel >> File Transfer .

5 Select the given options appropriately.

6 Click **Save**.

EventTracker creates a DLA system instance with the Agent name appended by **"-DLA"** (For example: Mcloon-DLA) and transfers filtered events and other log files through the DLA channel.

Figure 335
System Manager

The screenshot shows the 'Systems' window in EventTracker. It has a search bar at the top with a 'Go' button. Below the search bar, it says 'All Domain Computers' and 'Managed systems: 65'. There are three tabs labeled '1', '2', and '3'. The main table lists various computers with columns for Computer, Type, EventTracker Port, EventTracker Version, Change Audit Version, and Asset value. The computer 'MCL00N-DLA' is highlighted in red.

Computer	Type	EventTracker Port	EventTracker Version	Change Audit Version	Asset value
ALICE-II	XP Pro	--	--	--	Low
BALOO	XP Pro	--	--	--	Low
CHARLIE-II	XP Pro	--	--	--	Low
MCL00N	XP Pro	14505	7.2 - Build 25	7.2 - Build 25	Undefined
MCL00N-DLA	XP Pro	14505	7.2 - Build 25	7.2 - Build 25	Undefined
ELR	2003	--	--	--	High
ESXVCSERVER	2003	--	--	--	High
ESXWIN2K3VM4	2003	--	--	--	High
ESXWIN2K3VM5	2003	--	--	--	High
ESXWIN2K864VM2	2008	--	--	--	High
ESXWIN2K8R2VM6	2008 R.2	--	--	--	High
EXCHTEST	2003	--	--	--	High

Figure 336
Log Search result
page

To view filtered out events, click the navigation link **Search**. EventTracker opens the **Log Search** window >> type the DLA system name in the search field >> click **Go**.

The screenshot shows the 'Log search - Windows Internet Explorer' window. It has a search bar at the top with a 'Go' button. Below the search bar, it says 'Total event count: 19,341'. The main table lists search results with columns for ID, Log Time, Event Properties, and Event Description. The search results are for 'mcl00n dla' and show events from 1/10/2012 2:15:35 PM to 1/11/2012 2:15:35 PM.

ID	Log Time	Event Properties	Event Description
1	1/11/2012 01:19:32 PM	Event ID: 577 Log Type: Security Event Type: Audit Success Category: 4 Source: Security Domain: NT AUTHORITY Computer: MCL00N-DLA User: SYSTEM	Privileged Service Called: Server: NT Local Security Authority / Authentication Service Service: LsaRegisterLogonProcess() Primary User Name: MCL00N5 Primary Domain: TOONS Primary Logon ID: (0x0,0x3E7) Client User Name: MCL00N5 Client Domain: TOONS Client Logon ID: (0x0,0x3E7) Privileges: SeTcbPrivilege
2	1/11/2012 01:19:19 PM	Event ID: 577 Log Type: Security Event Type: Audit Success Category: 4 Source: Security Domain: NT AUTHORITY Computer: MCL00N-DLA User: SYSTEM	Privileged Service Called: Server: NT Local Security Authority / Authentication Service Service: LsaRegisterLogonProcess() Primary User Name: MCL00N5 Primary Domain: TOONS Primary Logon ID: (0x0,0x3E7) Client User Name: MCL00N5 Client Domain: TOONS Client Logon ID: (0x0,0x3E7) Privileges: SeTcbPrivilege
3	1/11/2012 01:19:18 PM	Event ID: 3223 Log Type: System Event Type: Information Category: 2 Source: EventTracker Domain: TOONS Computer: MCL00N-DLA User: sonal	Socket CREATED: Type: TCP Status: New Local Address: mcl00n.Toons.local Local Port: 2219 Remote Address: MAA03S04-IN-F18.1E100.NET Remote Port: 80 (http) Connection State: ESTAB Process ID: 2380 Process Name: iwebmon.exe Image File Name: C:\Program Files\Prism Microsystems\StatusTracker\iwebmon.exe
4	1/11/2012 01:19:18 PM	Event ID: 3223 Log Type: System Event Type: Information Category: 2 Source: EventTracker Domain: TOONS Computer: MCL00N-DLA User: sonal	Socket CREATED: Type: TCP Status: New Local Address: mcl00n.Toons.local Local Port: 2229 Remote Address: SAFARI.TOONS.LOCAL Remote Port: 135 (epmap)

Search results for: mcl00n dla, Time range : 1/10/2012 2:15:35 PM - 1/11/2012 2:15:35 PM

Assessing Configuration

This feature helps to validate actual system security and configuration against NIST recommendations. If enabled, EventTracker Agent listens for requests for assessment, conducts the assessment, and returns the results via the Security Content Automation Protocol (SCAP).

To enable configuration assessment

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** dropdown, and then click **Windows Agent Config**.
- 3 Select the system from the **Select System** hyperlink.
- 4 Click the **Config Assessment** tab.

Figure 337
Config Assessment
tab

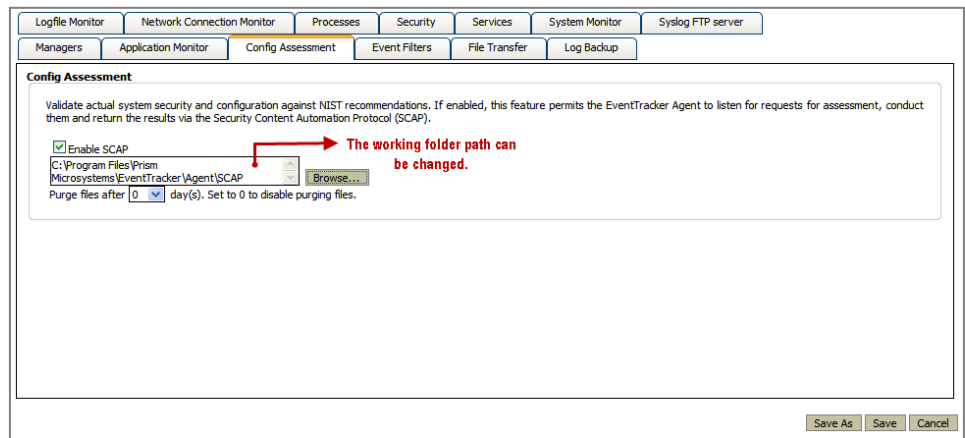


Table 110

Field	Description
Enable SCAP	If enabled, EventTracker Agent evaluates the configuration policy against the system and sends back the result to the Manager.
Working folder	EventTracker Agent stores the temporary files in this folder before it sends the result to the Manager.
Purge files after	EventTracker Agent purges the contents of the temporary folder after this configured number of days.

- 5 Configure appropriately.
- 6 Click **Save**.

Applying Configuration Settings to Specified Agents

This option enables you to apply the current configuration settings of the selected system to other specified Agents from one centralized location.

Only the saved configuration settings can apply to the specified

To apply configuration settings to specified Agents

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** dropdown, and then click **Windows Agent Config**.
- 3 Select the system from the **Select System** hyperlink.
- 4 Click **Apply this configuration to agents** button.

EventTracker displays the 'Apply client configuration across enterprise' dialog box.

Figure 338
Apply client
configuration across
enterprise

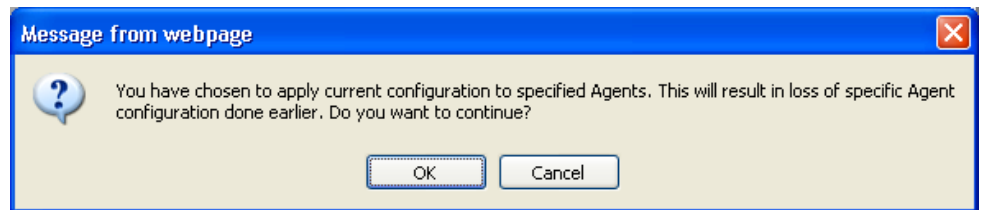
Table 111

Available options	Description
Apply All Settings	Select this option to apply all settings including the default and modified settings.
Apply Only Modified	EventTracker selects this option by default. Leave as it is to

Available options	Description
Settings	apply only the modified settings.
Apply Only Selected Settings	Select this option to apply only the selected settings made under respective configuration options. EventTracker enables the checkboxes. Select appropriate configuration options and then click Apply .

- 5 Select a system group.
EventTracker displays the managed systems associated with the selected group.
- 6 Select the systems.
- 7 Click **Apply**.
EventTracker displays confirmation message.

Figure 339



- 8 Click **OK**.
EventTracker displays the message 'Settings applied successfully'.
- 9 Click **OK**.
- 10 Click **Save**.

Backing up Current Configuration

This option enables you to back up the current configuration settings.

To back up the current configuration settings

- 1 Open **EventTracker Control panel**, and then click **EventTracker Agent Configuration**.
EventTracker, by default displays the **Managers** tab.
- 2 Select the system from the **Select Systems** drop down list.
- 3 Click the **File** menu, and then click the **Backup** option.
EventTracker, by default displays the 'Backup Current Configuration' dialog box.
- 4 Select the path where you want to backup the current configuration settings.
- 5 Enter the file name in the **File name** field.
The valid file extension is '*.ini'.

- 6 Click **Open**.
EventTracker displays the 'EventTracker Agent Configuration' message box.
- 7 Click **OK**.

Protecting Agent Configuration Settings

This option enables you to protect the EventTracker agent configuration settings. You can allow local system or specified remote system(s) to modify the agent configurations. Once the agent configuration is protected, then the agent settings will be modified only by local system and/or specified IP addresses.

To protect the Agent configuration settings for local and Agent systems

- 1 Log on to **EventTracker Enterprise**.
- 2 Click the **Admin** dropdown, and then click **Windows Agent Config**.
- 3 Select the system from the **Select System** hyperlink.
- 4 Click the **Security** tab.

EventTracker displays **Agent Configuration Protection** pane.

Figure 340

In Windows Agent Console, 'Security' option is available under the File menu.

Table 112

Field	Description
Enable protection for agent configuration	Select this checkbox to enable other options in this dialog box.
Settings can be modified on the following system(s)	Local System: Select this checkbox to protect the current configuration settings only for the local system. Other users cannot modify your settings from their machines.
	Enter IP Address: Select this checkbox to protect the current configuration settings for other machines.

Field	Description
	<p>IP Address:</p> <p>Type the IP address(es) in this dialog box.</p> <p>You can configure the current configuration settings up to five IP addresses.</p> <p>The IP addresses specified in this field can modify the agent configuration settings.</p>
Remedial Action	Select the checkbox to enable the remedial action.

- 5 Select the **Enable protection for Agent configuration** checkbox.
- 6 Select/enter appropriately in the relevant fields.
- 7 Click the **Save** button.

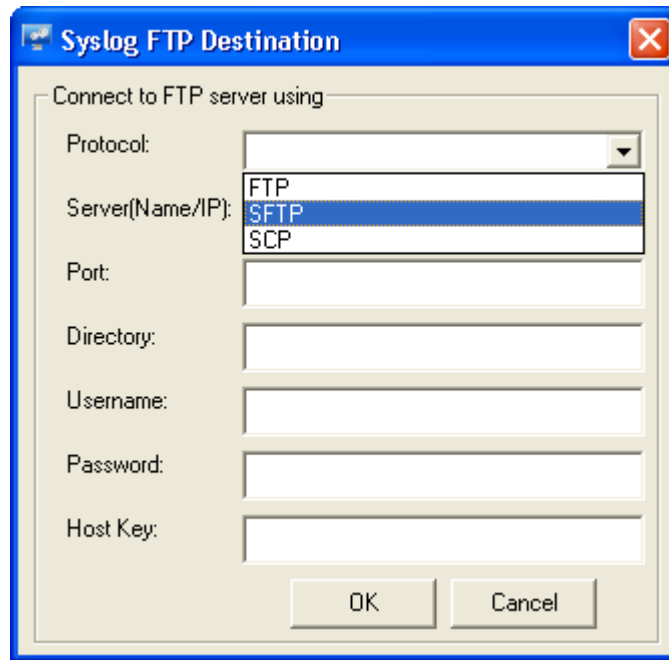
Syslog FTP Sever

This new feature is introduced to transmit windows events from local systems, as text files containing syslog messages.


To transfer Windows events as syslog messages

- 1 Open **EventTracker Control Panel**.
 - 2 Double click **EventTracker Agent configuration**.
 - 3 Click **Syslog FTP server** tab.
 - 4 Click the **Add** button.
- EventTracker opens Syslog FTP destination pop-up window.

Figure 341
Syslog FTP
Destination



The image shows a Windows-style dialog box titled "Syslog FTP Destination". It contains several input fields and a dropdown menu. The "Protocol" dropdown menu is open, showing three options: "FTP", "SFTP", and "SCP", with "SFTP" currently selected. Below the dropdown are text boxes for "Server(Name/IP)", "Port", "Directory", "Username", "Password", and "Host Key". At the bottom of the dialog are "OK" and "Cancel" buttons.

- 5 Select the **Protocol** name, from the protocol dropdown list.
If you select protocol as FTP then port number 21 will be selected by default in the **Port** field.
If you select protocol as SFTP/SCP, then the **port number 22** will be selected by default in the **Port** field.
- 6 Enter the server name or IP address in **Server (Name/IP)** field, where the syslog messages to be transferred.
- 7 Enter the location in **Directory** field, where the files need to be transferred.
- 8 Provide the appropriate **Username** and **Password**.
- 9 Enter the host key in the **Host key** field, which is provided by the System Administrator.
Host Key option is available only for SFTP/SCP.
- 10 Click **OK**.
The server details can be seen in the **FTP server(s)** field.
- 11 Click **Send winsyslog Events via File Transfer** checkbox to allow the file transfer to happen.
- 12 To send other log files, click Send other log files checkbox, and then click the  browse button.
EventTracker displays **Browse for folder** pop-up window.

- 13 Select the log file folder, and then click **Ok**.

(OR)

Click the location where you want to create a folder, and then click **Make a New Folder** button.

EventTracker creates new folder under the selected location. Right click and rename the **New folder**, and then click **Ok**.

All the files placed in this folder will be transferred to the configured manager.

To edit server details

- 1 Select the server details which you want to edit from **FTP server(s)** list, and then click the **Edit** button.

EventTracker Manager opens Edit destination pop-up window.

- 2 Make the appropriate changes, and then click **OK**.

To remove server details

- 1 Select the server details which you want to remove from **FTP server(s)** list.
- 2 Click the **Remove** button.

To format syslog message

This option helps you to select the event properties, which needs to be included in the output syslog message, to set the replacement character for the new line, and to add the severity and facility conditions to the output message.

- 1 Open EventTracker Control panel.
- 2 Click the **syslog FTP server** tab/ click **Manager** tab.
- 3 Click **Message Options** button.

EventTracker displays **Syslog Message options** pop-up window.

Figure 342
Syslog message
options

Syslog Message Options

RFC 3164 Syslog Facility Settings

Log Type	Event Type	Cate...	Eve...	Source	User	Description	RFC 3164 Facility Name
Application		0	0				[1] user-level messages
Security		0	0				[4] security/authorization mes...
System		0	0				[0] kernel messages

New Edit Delete

RFC 3164 Syslog Severity Configuration

Log Type	Event Type	Cate...	Eve...	Source	User	Description	RFC 3164 Severity Name
	Information	0	0				[6] Informational: informational...
	Error	0	0				[1] Alert: action must be taken...
	Warning	0	0				[3] Error: error conditions
	Audit Failure	0	0				[2] Critical: critical conditions
	Audit Success	0	0				[5] Notice: normal but significa...

New Edit Delete

Syslog Description Settings

Select event properties to be included in the description of the syslog message. Select appropriate Event format options to convert new lines in the Windows event descriptions.

Event Properties

☒ Event ID ☒ Event Type ☒ Source ☐ Description
☒ Category ☒ Log Type ☒ User

Syslog Format

Replace new lines (CR LF) with: Space

☐ Insert Prefix

OK

Top pane displays list of facility conditions and bottom pane displays severity condition list. There is no limit for number of conditions to be added.

- In **RFC 3164 Syslog Facility Settings** pane, click the **New** button.
EventTracker displays Event details pop-up window.

Figure 343
Event Details

Windows Event Details (empty field implies all matches)

Log Type :

Event Type : Event ID :

Category : Match in User :

Match in Source :

Match in Event Descr :

"Match in Event Descr" field can take multiple strings seperated with && or ||.
 - && stands for AND condition. - || stands for OR condition.
 Note:
 If you want to make a match on any of the special characters, like "\", "^", "\$", etc... ,
 then in the search string prefix this
[For more information click here.](#)
 Example: "\\" for a "\" and "\\^" for a "^".

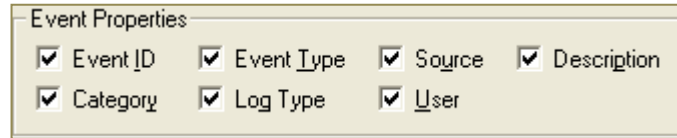
Syslog Details
 RFC 3164 Syslog facility type:

OK Cancel

- 5 Enter/select the appropriate event properties.
- 6 In the Syslog Details pane, select appropriate syslog facility type from **RFC 3164 Syslog facility type** dropdown.
- 7 Click **OK** button.
- 8 In **RFC 3164 Syslog Severity Settings** pane, click the **New** button.
EventTracker displays Event details pop-up window.
- 9 Enter/select the appropriate event properties.
- 10 In the Syslog Details pane, select appropriate syslog facility type from **RFC 3164 Syslog Severity type** dropdown.

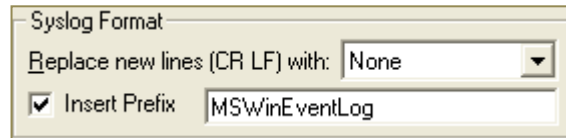
- 11 Click **OK** button.
- 12 In the **Event Properties** pane, select the event properties to be included in the description of the syslog message.

Figure 344
Event Properties



- 13 In syslog format pane, select new line spacing option from **Replace new lines (CR LF)** with dropdown.

Figure 345
Syslog Format



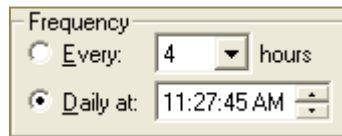
- 14 If you wish to prefix the EventId in description field then select the Insert prefix checkbox, and enter the prefix.
By default, **MSWinEventLog** will be selected as prefix.
- 15 Click the **OK** button.

To set file transfer frequency and purge transferred files

This option helps you to set the frequency to transfer the syslog files and to purge the transferred syslog files after the specified duration. For transferring events to both windows server and syslog receiver, file transfer frequency and purge duration will be configured in **File transfer tab**.

- 1 In EventTracker Agent configuration, select **File transfer** tab.
- 2 In the **Frequency** pane, set the frequency of file transfer.

Figure 346
Frequency

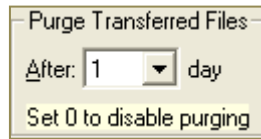


Select **Every – hours** option, to set file transfer to occur every configured hours.
(OR)

Select **Daily at** option, to set file transfer to occur daily at a particular time.

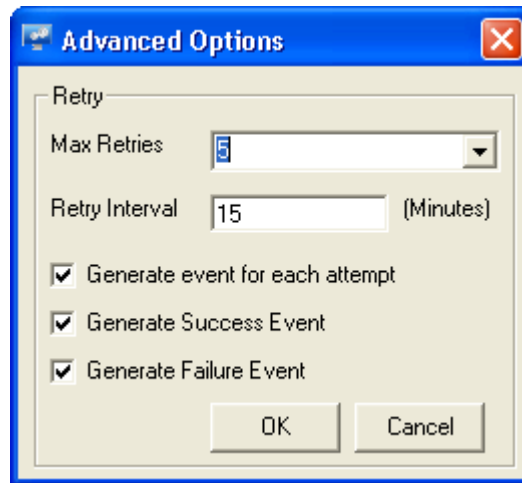
- 3 In **Purge Transferred Files** pane, select the number of days from **After – day** dropdown to purge the transferred files every configured day.

Figure 347
Purge Transferred
Files



- 4 Click the **Advanced** button.
EventTracker displays **Advanced options** tab.

Figure 348
Advanced Options



- 5 Select maximum retries from **Max Retries** dropdown in case of transfer failure.
Maximum 5 retries will be selected by default. If you select INFINITE retries from the dropdown, then EventTracker will keep on sending the syslog file after specified interval.
- 6 Enter the file transfer duration (in minutes) in **Retry interval** field.
By default, it will be set to 15 minutes.
- 7 Select/clear the appropriate checkbox.
All the three checkboxes are selected by default.
- 8 Click the **Ok** button.

To Transfer files immediately


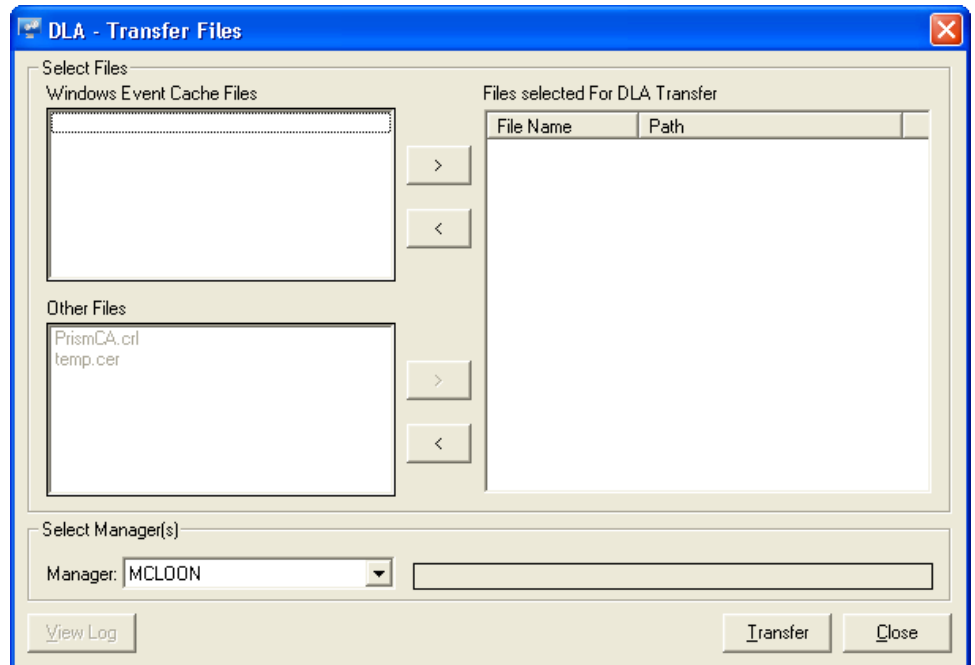
- 1 Open the File transfer tab, and then click **Send Now**  button.
EventTracker opens DLA-Transfer Files tab.

Figure 349
DLA Transfer Files



- 2 From **Windows Event Cache Files**, select the cache file to be transferred, and then click button.
The selected file will appear in the **Files selected for DLA transfer** list.
- 3 Likewise, select other files to be transferred from Other Files list, and then click button.
The selected file will appear in the **Files selected for DLA transfer** list.
- 4 To remove the file from selected files list, select the file to be removed in **Files selected for DLA transfer** list, and then click button.
- 5 Select the destination manager from **Manager** dropdown, and then click the **Transfer** button.

The files listed in **Files selected For DLA Transfer** list will transferred immediately.

Enabling Remedial Action

After enabling remedial actions at the Manager Console, you have to individually enable 'Remedial Action' on all the Agent systems. You can also include or exclude Agents from taking remedial actions.

- 1 Move to the Windows Agent Configuration page.
 - 2 Select the system from the Select **System** hyperlink.
 - 3 Click the **Security** tab.
 - 4 Select the **Remedial Action** checkbox.
 - 5 Click **Save**.
-

Generating System Report

System Report helps you keep track of Managed and Unmanaged systems. Filter option is provided to view the ports used by Managed systems.

To generate system report

- 1 Open the System Manager.
- 2 Click the **Admin** dropdown, and then select **Systems..**
- 3 Click the **System Report** button.

System Manager displays the System Report pop-up window.

Figure 350
System Report

System Report

View reports

☐ View report of all systems of any type, on any port in any group

Show only

System Status: ☒ Managed ☐ Unmanaged ☐ All

Select by

☒ System Type ☐ Group ☐ Port Number

System Type: All systems

Include systems

☐ Offline ☐ Syslog ☐ Netflow

Sort by

Computer

Generate Report Close

Note

EventTracker disables the **Port Number** option, if you select the **Unmanaged** option.

Viewing Reports

This option helps to view reports of all systems irrespective of ports or groups.

To view reports

- 1 Select the **View report of all systems of any type, on any port in any group** checkbox.
- 4 Click **Generate Report**.
System Manager displays the File Download pop-up window.
- 2 Click **Open** to view the Excel file.
(OR)
Click **Save** to download and save the file in a safer location.

Managed System Report

This option helps you generate O/S wise, group wise and port wise report.

To generate system type wise report

- 1 Select the **Managed** option.
- 2 Select the **System Type** option to view Managed systems by operation systems.
- 3 Select an O/S type from the **System Type** drop-down list.
EventTracker populates this drop-down list with only the operating systems installed on the Managed systems.
- 4 Click **Generate Report**.
EventTracker displays the File Download pop-up window.

Note



System Type **Unknown** represents non-Windows operating systems.

To generate group wise report

- 1 Select the **Managed** option.
- 2 Select the **Group** option to view Managed systems by group.
- 3 Select a group from the **Group** drop-down list.
EventTracker populates this drop-down list with all discovered enterprise system groups.
- 4 Click **Generate Report**.

To generate port wise report

- 1 Select the **Managed** option.
- 2 Select the **Port Number** option to view Managed systems by port.
- 3 Select a port from the **Port Number** drop-down list.
EventTracker populates this drop-down list with all configured ports.
- 4 Click **Generate Report**.

Unmanaged System Report

This option helps you generate O/S wise and group wise report.

To generate system type wise report

- 1 Select the **Unmanaged** option.

- 2 Select **System Type** option to view unmanaged systems by operating systems.
 - 3 Select an O/S type from the **System Type** drop-down list.
 - 4 Click **Generate Report**.
-

To generate group wise report

- 1 Select the **Unmanaged** option.
 - 2 Select the **Group** option to view unmanaged systems by group.
 - 3 Select a group from the **Group** drop-down list.
 - 4 Click **Generate Report**.
-

All System Report

This option helps to generate O/S wise, group wise and port wise Managed / Unmanaged system report.

Chapter 17

Agentless Monitoring of Windows Systems

In this chapter, you will learn how to:

- [Add Systems for Agentless Monitoring](#)

Agentless Monitoring

In cases where it is not possible or desirable to install the EventTracker Windows Agent, EventTracker can be configured to periodically poll the target computers over the network to collect new event log entries since the last poll.

Pros

- No agent to deploy – Simpler product deployment. There is lesser effort during planning, deployment, and upgrade.

Cons

- Increased network load – Depending on the selected polling cycle and level of event generation, network load is greater.
- Greater dependency, more critical points of failure – The Console becomes critical since it is polling target machines. Network choke points can impact performance.
- Real-time notification not possible – The earliest notifications that can be sent depends on where the Console is in its polling cycle.
- Limited to operation within a domain – The Console and target machine must be in the same domain so that domain privileges are preserved.
- Performance monitoring – this feature is not available.
- Application monitoring – this feature is not available.
- Software install/removal monitoring – this feature is not available.
- Service monitoring – this feature is not available.
- Monitoring external log files – this feature is not available.
- Host based intrusion detection – this feature is not available.
- Non-domain topologies not supported – this feature is only available when the Console and target machine are in the same Windows domain.

Adding Systems for Agentless Monitoring

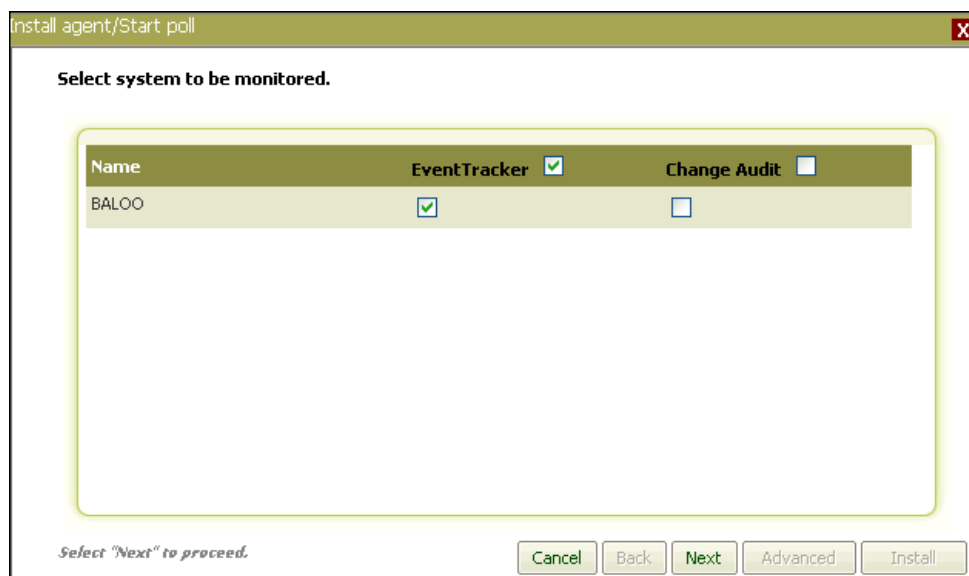
This option enables you to add systems from where you want to collect events periodically. The resource (CPU/memory/disk) usage, log file monitoring, and other agent-required features are disabled, in the agent-less monitoring systems. Additionally, the service account of the local agent should have administrative privileges on all the systems that are added for collecting events.

To add systems for Agentless monitoring

- 1 Open the **System Manager**.

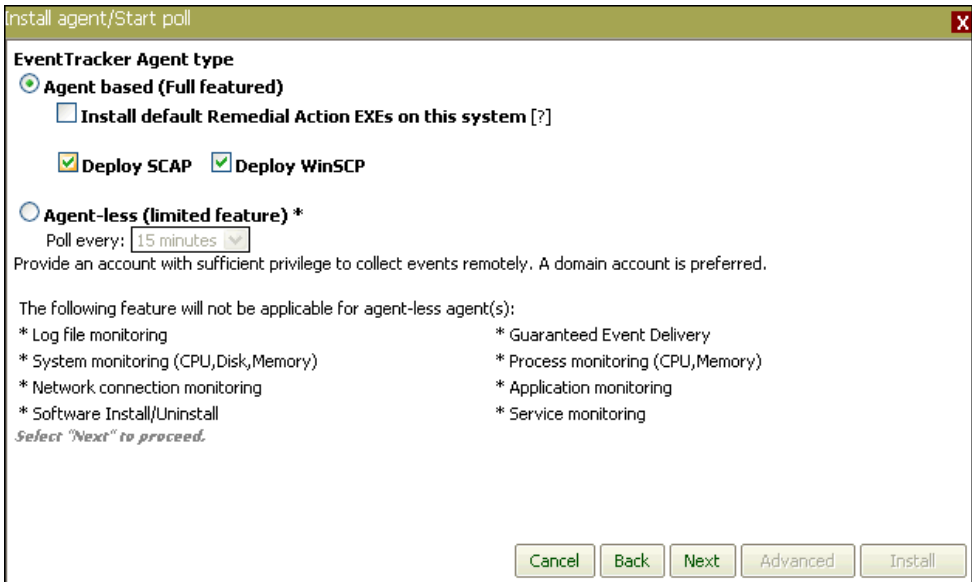
- 2 Right click the system group to which the target system is a member.
System Manager displays the shortcut menu.
- 3 From the shortcut menu, click **Install agent/Start poll**.
(OR)
- 1 Click the system that you wish add for agent less monitoring.
System Manager displays the shortcut menu.
- 2 From the shortcut menu, click **Install agent/Start poll**.
System Manager displays the Install Agent/Start poll window.

Figure 351
Add Agent



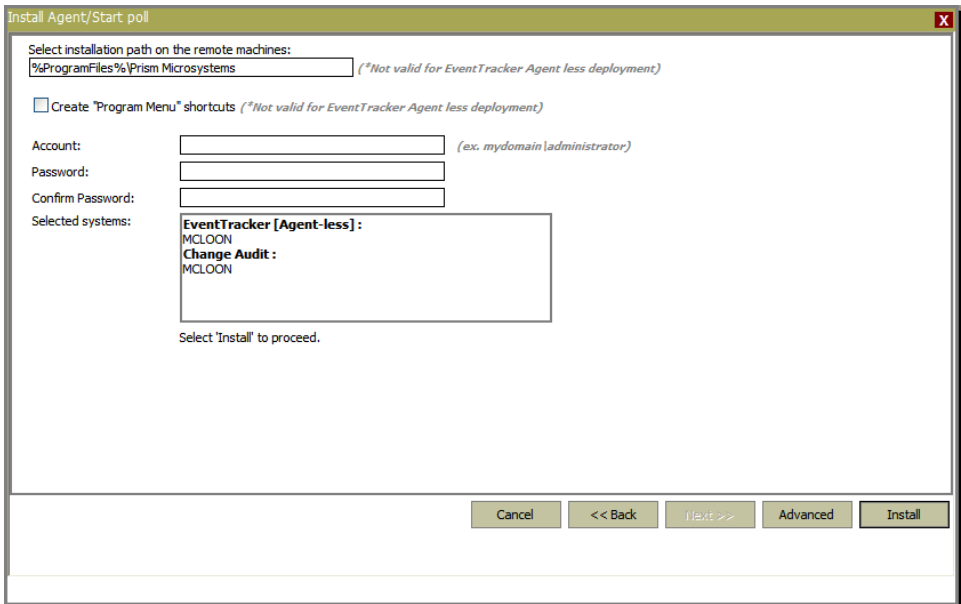
- 3 Select the **EventTracker** checkbox.
Selecting this option will not install Agent on the remote system; rather enable EventTracker Manager to poll the remote system.
- 4 Select the **Change Audit** checkbox to enable Change Audit manager to poll the remote system
Click [here](#) to know more about **Change Audit** Install.
- 5 Click **Next**.
- 6 Select the **Agent-less (limited feature)*** option.

Figure 352
Add Agent –
Installation path



- 7 Select the polling period from the **Poll every** drop-down list. EventTracker Manager polls the system at the configured interval.
- 8 Click **Next**.

Figure 353
Add Agent –
Installation path



- 9 Select the Create 'Program Menu' shortcuts to create Program menu shortcuts on the target system.
- 10 NOTE: This option is valid only for EventTracker agent based monitoring.

11 Type valid user credentials in **Accounts**, **Password**, and **Confirm Password** field.

Note

To set a more specific configuration, click **Advanced** (OR) click **Install** to install the Agent.

12 Click **Advanced**.

System Manager displays the Install Agent window to select the default or custom .ini file.

Figure 354
Agent Configuration

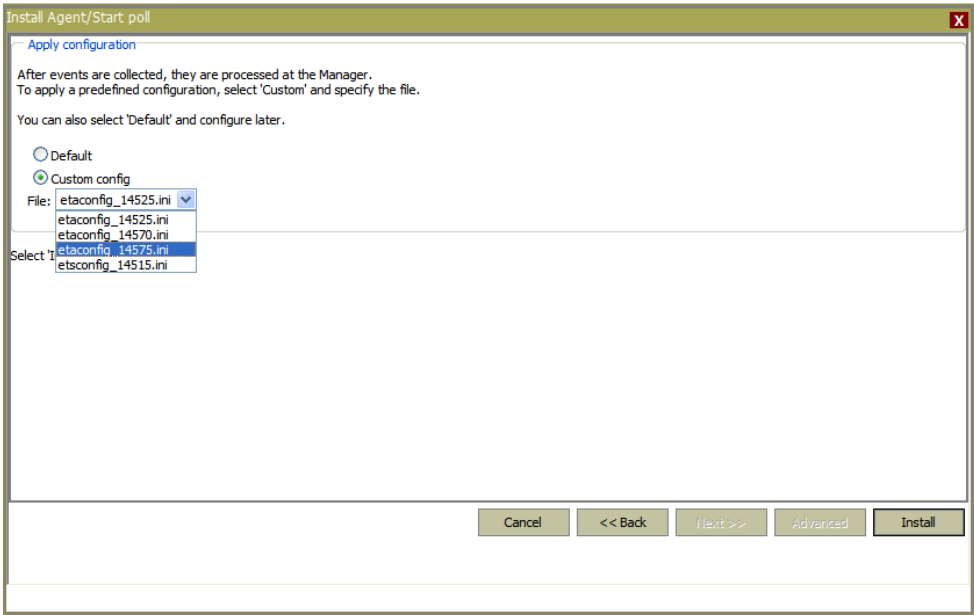


Table 113

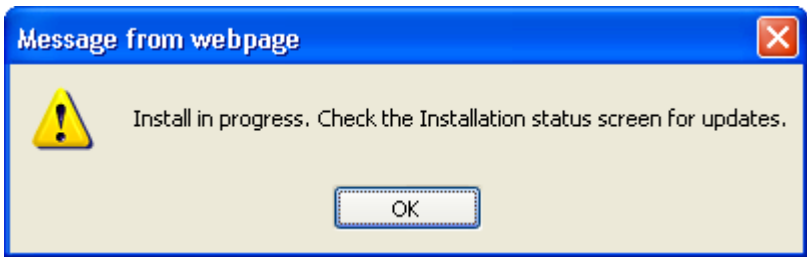
Field	Description
Default	Select this option to set the default agent configuration. The default configuration will track all events.
Custom Config	Select this option to apply a different configuration. The File field is enabled. Type the path of the ini file. The file extension should be in the EventTracker Agent .ini format and would be a previously saved configuration file.

13 Click appropriate agent configuration settings.

14 Click **Install**.

System Manager starts adding the system and displays the message box with appropriate message.

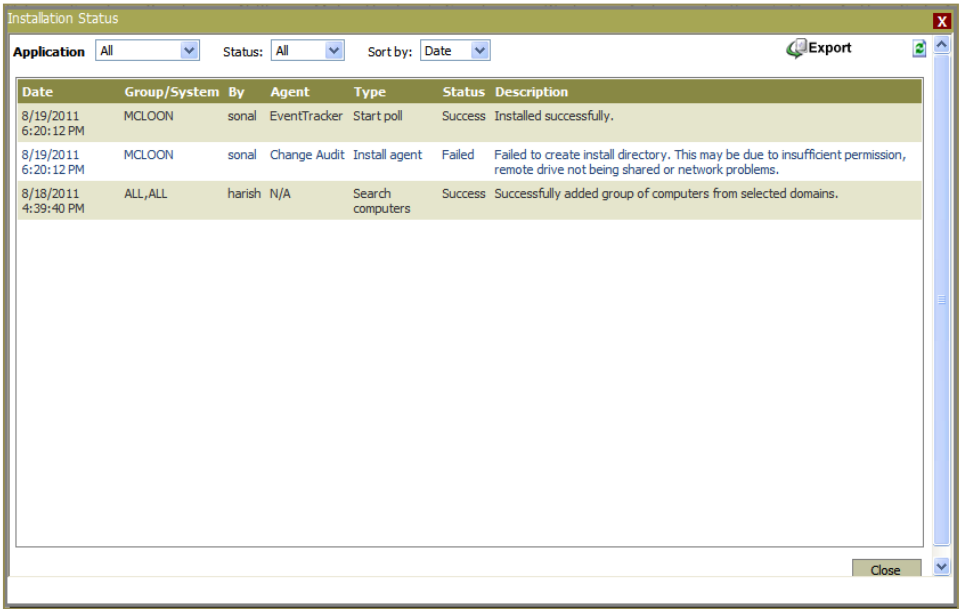
Figure 355
Add Agent –
Successful
installation
message



15 Click **OK**.

EventTracker displays Installation Status window.

Figure 356
Installation Status



16 Click **Refresh** button to see the updated status.

Note

To view the installation status, click the **Installation Status** button on the System Manager.

Agentless monitoring cannot be deployed from **Pre-Vista** to **Post vista** systems.

Figure 357
Installation Status

Date	Group/System	By	Agent	Type	Status	Description
9/7/2012 12:14:01 PM	BALOO	deepa	EventTracker	Install agent	Failed	Copying files to the remote system failed.
8/31/2012 10:46:28 AM	CACOFONIX	deepa	EventTracker	Install agent	Failed	Copying files to the remote system failed.
8/30/2012 5:37:45 PM	EXCHTEST	deepa	EventTracker	Install agent	Failed	Copying files to the remote system failed.

Chapter 18

EventVault Manager

In this chapter, you will learn how to:

- [Configure EventVault](#)
- [Verify EventBox Integrity](#)

About EventVault

EventTracker stores all received events in EventVault, an optimized and high performance event warehouse that is purpose-built for efficient storage and retrieval of event logs. All collected events are compressed (over 90% compression ratio), encrypted, and sealed with a SHA-1 signature to prevent potential tampering.

EventTracker Scheduler Service

Firewall settings (Example: Windows Firewall): When the EventTracker Scheduler service tries to access CAB files on the remote machine, the Firewall may deny access to the remote machine. Allow Firewall to permit EventTracker Scheduler service to access CAB files on the remote machine.

Collection Master and Collection Point communicate through port **14507**.

You can also add EventTracker Scheduler service to Exceptions Programs and Services list in Windows Firewall by doing the following:

- 1 Open **Windows Firewall settings** window.
- 2 Click the **Exceptions** tab.
- 3 Click **Add Program**.
- 4 Click **Browse** and add the EventTracker Scheduler service to Programs and Services list.

EventTracker Scheduler service – Collection Master Console

EventTracker Scheduler service at Collection Master Console behaves as a server and will always be in 'Listen' mode. Any number of Collection Points can be connected to Collection Master.

EventTracker Scheduler service – Collection Point Console

EventTracker Scheduler service at Collection Point Console wakes up once in 30 seconds and launches CollectionPointConfig.exe. This exe in turn will query the configuration database for new CAB files to be sent to the Collection Master.

Viewing CAB Files

This option helps you view CAB files for a specific period.

To view CAB files

- 1 Click the **Admin** hyperlink, and then click **EventVault**.
By default, EventVault Manager selects the **Show All** option and displays all the CAB files.
 - 2 Select the **Older than** option to view CAB files older than a specific period.
 - 3 Select/enter date and time from Date and Time control.
 - 4 Select the port number from **Port No.** dropdown.
By default, all ports option is selected to view all the available cab files.
 - 5 Click **Show**.
EventVault Manager displays the CAB files older than the specified period and/or from specific port
 - 6 Select the **From** option to view CAB files for a specific period.
 - 7 Select/enter date and time from Date and Time control.
 - 8 Click **Show**.
EventVault Manager displays the CAB files for the specified period and/or from specific port.
-

Configuring EventVault

This option enables you to configure the EventVault Manager to archive the events from EventTracker database. EventBoxes are created automatically based on two criteria,

- When the Cache db reaches 50 MB
OR
- EventVault Schedule frequency set by selecting the number of hours from the EventVault Frequency drop-down list on the EventVault Manager Configuration window.

To configure EventVault Manager

- 1 Open the EventVault Manager.
- 2 Click **Configuration**.
EventVault Manager displays the **Configuration** pop-up window.

Figure 358
Configuration dialog
box

Configuration

Vault Storage Folder

C:\Program Files\Prism Microsystems\EventTracker\Archives

EventVault Frequency

Force CAB file creation every:

24

Hrs

Archives will be created once in configured number of hours or when cache size exceeds 50Mb*

Purge

Archives will be purged after configured number of days:

☐ Purge Archives older than:

days

Ok

Cancel

Table 114

Field	Description
Vault Storage Folder	Displays EventVault Storage folder path. The path of the storage folder can be changed in the EventTracker control panel >> EventVault Warehouse Manager.
Force CAB file creation every	Archives will be created once in configured number of hours or when cache size exceeds 50 Mb.
Purge Archives older than	Select this checkbox and enter the number of days to retain CAB files. CAB files will be purged after the specified number of days. By default, EventVault Manager retains CAB files forever.

- 3 Type/select appropriately in the relevant fields.
- 4 Click **OK**.

Note

EventTracker saves the archive files in the selected location with the .cab extension.

Verifying EventBox Integrity

This option enables you to verify contents of the EventBox are intact. This will calculate a SHA1 hash value on the EventBox contents and compare with the original value.

While verifying the integrity of an EventBox, EventVault Manager performs the following actions

- The SHA1 checksum of the selected archive is regenerated.

- This new checksum is compared with the older (existing in the database) checksum.
- If the two checksums do not match then an error message is displayed indicating that the data has been tampered.
- If the two checksums match then it means that the data is intact.

To verify EventBox integrity

- 1 Open the EventVault Manager.
- 2 Select the CAB file(s) from the **Available EventBoxes** list.
- 3 Click **Verify**.

After verifying the integrity, EventVault Manager displays the ArchIntegrity report in the Notepad.

Viewing CAB Files by Port Number

This option helps you view CAB files by port number.

To view CAB files by port number

- 1 Open the EventVault Manager.
- 2 Select **Older than** or **From, To** option.
- 3 Set the time range.
- 4 Select a port number from the **Port No** drop-down list.
- 5 Click **Show**.

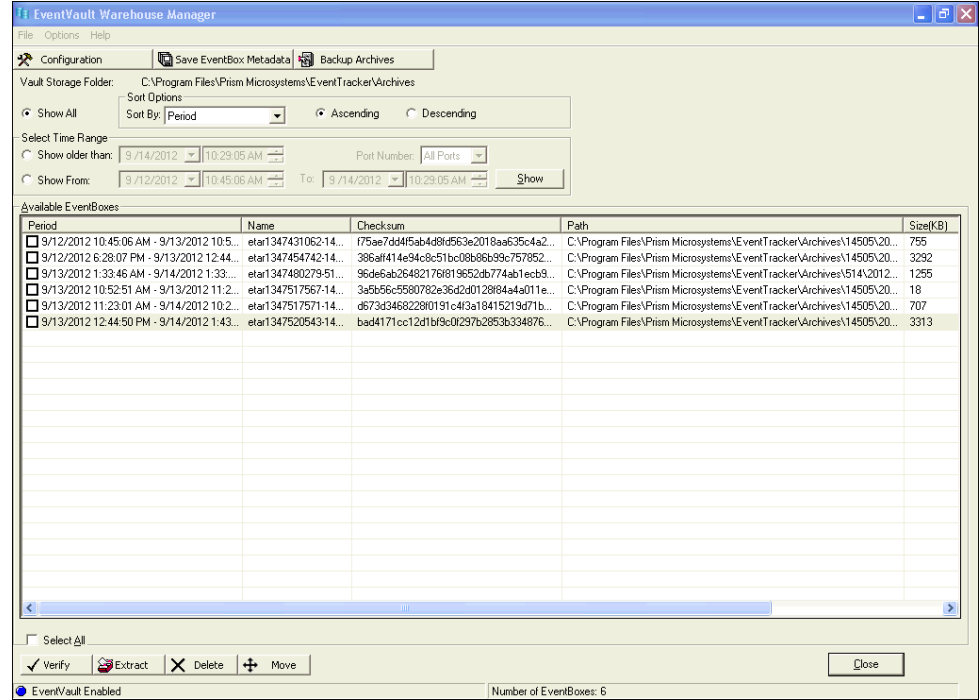
EventVault Warehouse Manager displays the CAB files of the selected port for the selected time range.

Note



Port Number drop-down list lists all ports configured, Default and VCP. Had you appended legacy CAB files (v 6.0 and earlier), select the 0-Legacy option. Port numbers were not appended to the names of Legacy CAB files as shown in the following figure.

Figure 359
Legacy EventBoxes



Chapter 19

Managing Category Groups and Categories

In this chapter, you will learn how to:

- [Manage Category Groups](#)
- [Manage Categories](#)
- [Add Categories as Alerts](#)

Managing Category Groups

A set of relevant Categories can be organized under a Group.

Creating Category Groups

This option enables you to organize Category groups whereby you can add, delete, and modify categories in that group.

To create a Category group

- 1 Click the **Admin** hyperlink, and then click **Category**.
- 2 Right-click **All Categories** or any other Category group.
EventTracker displays the shortcut menu.
- 3 From the shortcut menu, click **New Group**.

Note



If you select any other group than **All categories**, then the new group you create will be created as a sub-group under the group which is indicated in the **Parent Node** field.

Table 115

Field	Description
Parent Node	Name of the parent group under which EventTracker adds the newly created group as a sub-group.
Enter Group name	Type the name of the group.

- 4 Type the name of the group in the **Enter Group Name** field.
- 5 Click **OK**.
EventTracker creates the group under the selected parent group.
- 6 Follow the same procedure to create sub-group(s).
- 7 Click Reports drop down, and select Operations.
EventTracker displays the newly added Category group under the selected parent group.

Modifying Category Groups

This option enables you to modify a Category group.

To modify a Category group

- 1 Right-click the group that you want to modify.
EventTracker displays the shortcut menu.
- 2 From the shortcut menu, choose **Edit Group**.
EventTracker displays the Edit Group page on the right pane.
- 3 Type appropriate group name in the **Enter Group Name** field.
- 4 Click **OK**.

Note



You cannot edit the name of the Parent Node.

Deleting Category Groups

This option enables you to remove a Category Group.

To remove a Category Group

- 1 Right-click the group that you want to delete.
EventTracker displays the shortcut menu.
 - 2 From the shortcut menu, Click **Remove Group**.
EventTracker displays the Confirmation message box.
 - 3 Click **OK** to remove or **Cancel** to abort.
-

Managing Categories

A set of relevant events can be grouped under a Category. For example, you can create a set of MS-Exchange events under one Category and use this Category to show all events that occurred in MS-Exchange. This is far easier and flexible than generic reports.

Creating Categories

This option enables you to organize categories in an ordered manner. You can create, modify, and delete the categories.

To create a Category

- 1 Right-click the groups where you want to add Categories.
EventTracker displays the shortcut menu.
- 2 From the shortcut menu, click **New Category**.
EventTracker displays the Category Details page on the right pane.

Table 116


Field	Description
Parent Group	The parent node under which the new category is created.
Event Category Name	Type the name of the event Category.
Description	Type a brief description of the event Category.
Show In	This field allows you to add the new category to be shown under the Operations, Security, and/or Compliance Tree. Any new category by default will be added under Operations.

- 3 Type appropriately in the relevant fields.
- 4 Click **Add** to add **Event Rule**.
EventTracker displays the Event Configuration pop-up window.

Table 117

Field	Description
Event Rule	
Event Type	Select an event type from the drop-down list. The option describes the types of events Error, Warning, Information, Audit Success, Audit Failure, Success, Critical, and Verbose.
Category	Type the category number in this field. This field supports numeric data type only.
Log Type	This field describes the options are System, Security, Application, DNS Server, File Replication, and Directory Service.
Event ID	Type the event ID number in this field. This field supports numeric data type only.
Source	Type the source in this field.
User	Type the user name in this field.

Field	Description
Match in Event Description	Type a sub-string of the description that needs to be matched.
More information	Type the additional information about the event category in this field.

Note

If a field is left blank, a wildcard match for that field is assumed. For example, leaving the user field blank implies that any value in that field is acceptable.

- 5 Type appropriately in the relevant fields.
- 6 Click **Add**.
- 7 Click **Save**.

Modifying Categories

This option helps you modify Categories.

To modify a category

- 1 Right-click the Category that you want to modify.
EventTracker displays the shortcut menu.
- 2 From the shortcut menu, click **Edit Category**.
EventTracker displays the Category Details page on the right pane.

Table 118

Field	Description
Parent Group	The parent node under which the category was created. This field is not editable.
Event Category Name	This field displays the event category name. This field is not editable.
Description	Type the event category description in this field.
Show In	This field allows you to add the category to be shown under the Operations, Security, and/or Compliance Tree. Any new category by default will be added under Operations.

- 3 To edit event details, select an event and then click **Edit**.
EventTracker displays the Event Configuration pop-up window.

- 4 Edit appropriately and then click **Save**.
 - 5 Click **Save** on the Category Details page.
-

Deleting Categories

This option enables you to delete a Category

To delete a Category

- 1 Right-click the Category that you want to delete.
EventTracker displays the shortcut menu.
 - 2 From the shortcut menu, click **Remove Category**.
EventTracker displays the Confirmation message box.
 - 3 Click **OK**.
EventTracker deletes the selected Category.
-

Deleting Event Rules

This option helps you delete Event Rules.

To delete event Rules

- 1 Right-click the Category that you want to edit.
EventTracker displays the shortcut menu.
 - 2 From the shortcut menu, click **Edit Category**.
EventTracker displays the Category Details page.
 - 3 Select the event rule that you want to delete.
 - 4 Click **Delete**.
EventTracker displays the Confirmation message box.
 - 5 Click **OK**.
EventTracker deletes the selected event rule.
 - 6 Click **Save** on the Category Details page.
-

Adding Categories as Alerts

This option enables you to add Categories as Alerts

To add Categories as Alerts

- 1 Right-click the Category that you want to add as Alert.
EventTracker displays the shortcut menu.
 - 2 From the shortcut menu, click **Add as Alert**.
EventTracker displays the Alert Management -> Event Details page.
Type appropriate details as explained in the [Add Custom Alerts](#) section.
-

Chapter 20

EventTracker Utilities

In this chapter, you will learn how to use:

- [Export Import Utility](#)
- [EventVault Warehouse Manager](#)
- [Append Archives Utility](#)
- [Event Traffic Analyzer](#)
- [EventTracker Windows Agent Management Tool](#)
- [License Manager](#)

EventTracker Desktop Control Panel

- Double-click the icons to open Maintenance and support tools.

Figure 360
EventTracker
Desktop Control
Panel

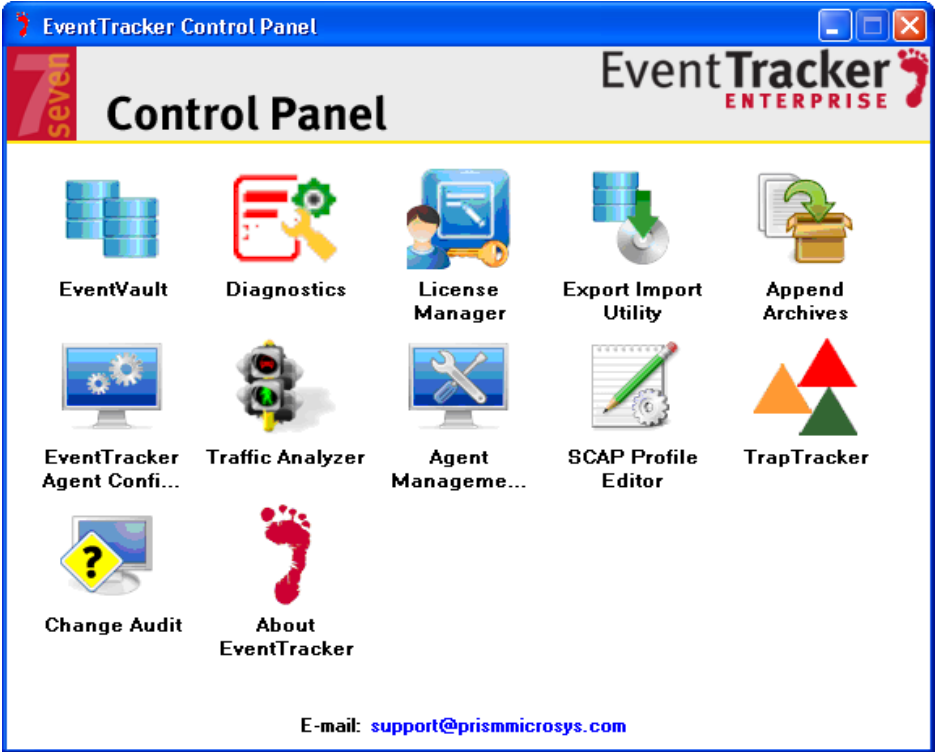








Table 119

Click	To
	Open EventVault Warehouse Manager.
	Open Diagnostic and Support Utility.
	Open License Manager.
	Open Export Import Utility.
	Open Append Archiver Utility. Use this utility to merge backup CAB files. Indexing is done automatically.
	Open EventTracker Agent Configuration window to configure EventTracker Windows Agent.







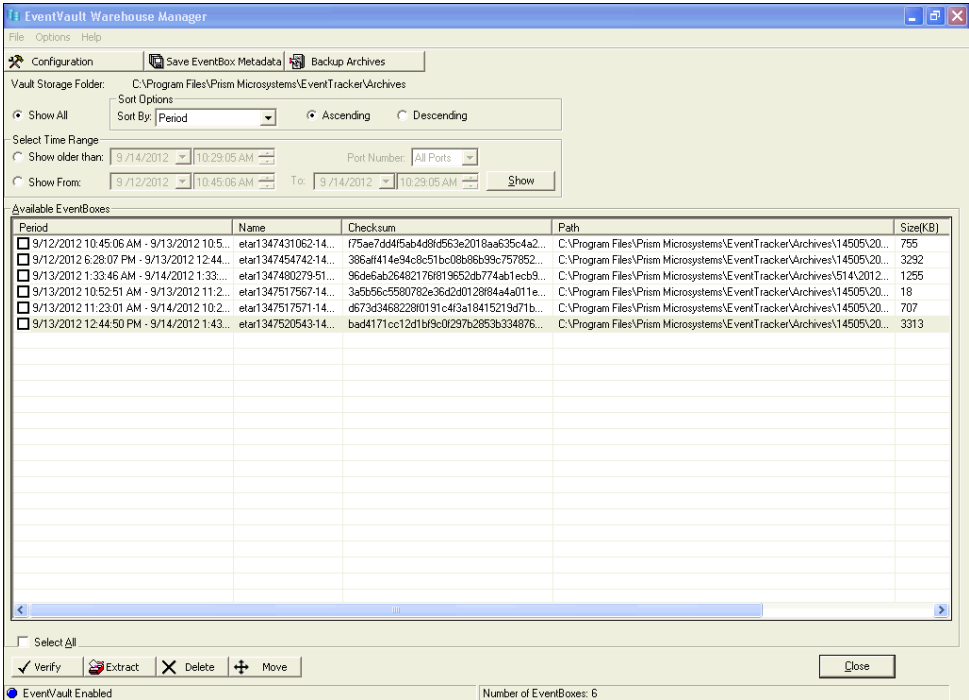
Click	To
	Open Traffic Analyzer to analyze event traffic.
	Open Windows Agent Management Tool.
 SCAP Profile Editor	Open SCAP profile editor.
	Open TrapTracker to manage traps received from SNMP enabled devices.
	Open Results Summary Console.
	View License Usage, patches applied and other details.

Table 120

EventVault Warehouse Managers

Figure 361
EventVault
Warehouse
Manager



Field

Description

Field	Description
Available EventBoxes	
Period	Time range of events stored in the CAB file.
Name	Name of the CAB file. etar1269949644-14505.cab etar – EventTracker Archive 1269949644 – Timeticks 14505 – Port number (through which the EventTracker Receiver service received the events) cab – File extension of cabinet files
Checksum	SHA 1 checksum number for tamper proof.
Path	Path of the folder where the archives are stored typically, EventTracker install path\ port number \ year \ month
Size (KB)	Size of the CAB file in KB.
Total Events	Total number of events accommodated in the CAB file.
Port Number	Port number through which the EventTracker Receiver service received the events.

Saving EventBox Metadata

This option enables you to save the archive summary in a text file. It helps you to locate particular .cab files to view, retrieve or extract events.

To save EventBox information

- 1 Double-click **EventVault** on the EventTracker Control Panel
 - 2 Select the archive file(s) from the **Available EventBoxes** list.
(OR)
Select the **Select All** checkbox to select all the archive files.
 - 3 Click **Save EventBox Metadata** on the toolbar.
EventVault Manager displays the Save As window.
EventVault Manager saves the EventBox Info in archive-info.txt file. You can also type the file name in the **File name** field.
 - 4 Select the path where you want to store the archive summary.
 - 5 Click **Save**.
-

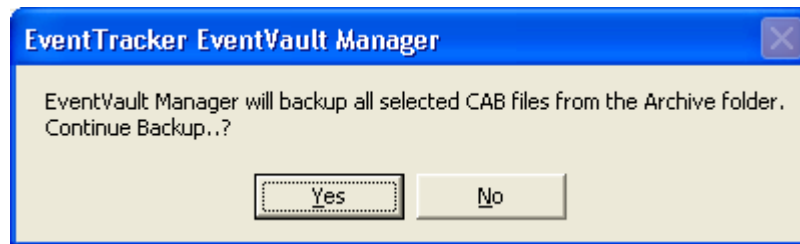
Backing up EventVault Data

This option enables you to backup EventVault data locally or remotely in a desired location for a long-term storage. It helps you to retrieve the backup data if the production archives are tampered.

To backup EventVault data

- 1 Open the EventVault Warehouse Manager.
- 2 Select the CAB file(s) from the **Available EventBoxes** list.
(OR)
Select the **Select All** checkbox to select all the archive files.
- 3 Click **Backup Archives** on the toolbar.
EventVault Warehouse Manager displays the confirmation message box.

Figure 362



- 4 Click **Yes**.
EventVault Warehouse Manager displays the Choose Directory window.
- 5 Select the folder where you want to store the event data.
- 6 Click **OK**.
EventVault Warehouse Manager displays the **ArchIntegrity** report in the Notepad after successful completion of backup.
If there is no archive file to back up, EventVault Warehouse Manager displays the message box with appropriate message.

Extracting EventBox Data

This option enables you to extract EventBox data into an MS Access database.

To extract EventBox data

- 1 Open the EventVault Warehouse Manager.
- 2 Select the CAB file(s) from the **Available EventBoxes** list.
- 3 Click **Extract**.
EventVault Manager displays the Choose Directory window.
- 4 Select the path where you want to store the event data.

5 Click **Save**.

After extracting the event data, EventTracker displays the ArchIntegrity report in the Notepad.

Note



EventVault Warehouse Manager saves the extracted .cab file in the selected location with .mdb file extension. You can view the database file using MS Access.

Moving CAB files

This option helps you move all or selected CAB files to a new location. After physically moving the CAB files, EventTracker updates the archive index. Moving the CAB files to a new location does not harm your scheduled reports. You can run on demand reports, define reports, and even configure new scheduled reports as you normally do.

To move CAB files

- 1 Open the EventVault Warehouse Manager.
- 2 Select the CAB files from the Available EventBoxes list.
(OR)
Select the **Select All** checkbox to select all the EventBoxes.
- 3 Click **Move**.
EventVault Warehouse Manager displays the confirmation message box.
- 4 Click **Yes** to proceed.
EventVault Warehouse Manager displays the Choose Directory dialog box.
- 5 Select the location (local or network) and then click **OK**.
EventVault Warehouse Manager moves all the selected files to the new location and displays the ArchIntegrity report in the Notepad.

Deleting an EventBox

This option enables you to delete an EventBox.

To delete an EventBox

- 1 Open the EventVault Warehouse Manager.
- 2 Select the CAB file(s) from the **Available EventBoxes** list.
- 3 Click **Delete**.

EventVault Warehouse Manager displays the Confirmation message box.

4 Click **OK**.

EventVault Warehouse Manager deletes the selected EventBox and displays the ArchIntegrity report in the Notepad.

Viewing CAB Files by Port Number

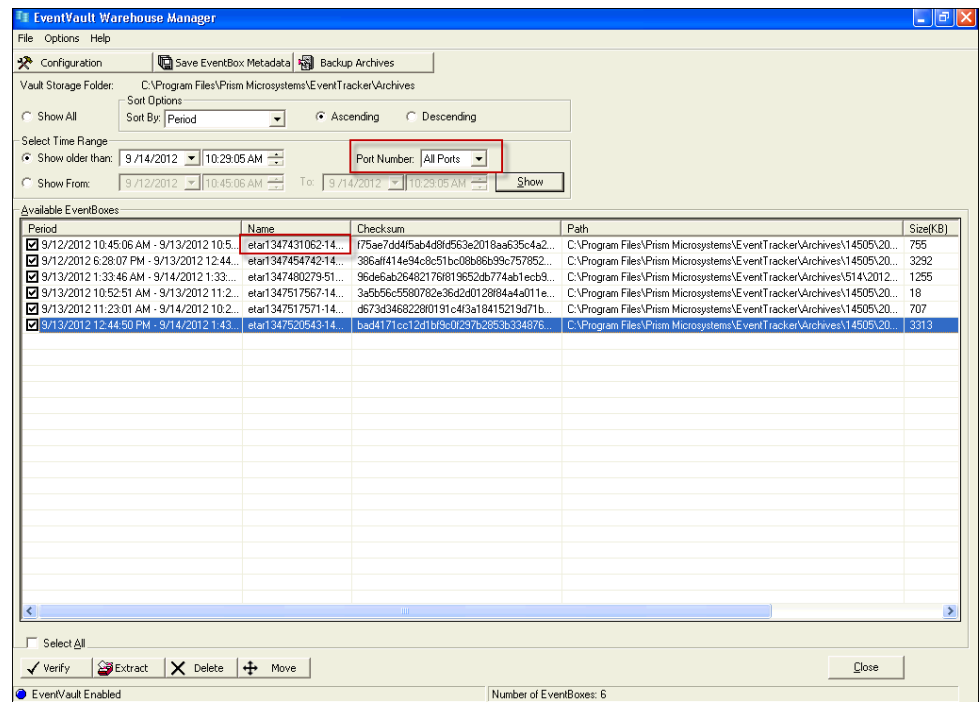
This option helps you view CAB files by port number.

To view CAB files by port number

- 1 Open the EventVault Warehouse Manager.
- 2 Select **Show older than** or **Show From** option.
- 3 Set the time range.
- 4 Select a port number from the **Port Number** drop-down list.
- 5 Click **Show**.

EventVault Warehouse Manager displays the CAB files of the selected port for the selected time range.

Figure 363
Append Archives
window



Note

Port Number drop-down list lists all ports configured, default and VCP. Had you appended legacy CAB files (v 6.0 and earlier), select the 0-Legacy option. Port numbers were not appended to the names of Legacy CAB files (See figure 410).

EventTracker Diagnostic Tool

Windows (optionally) adds the Diagnostics Tool as a Startup program after successful installation of EventTracker.

Diagnostics Tool alerts you if any problem occurs in the EventTracker.

Diagnostics data includes Product Information, System Information, License Information, Update Information, Service Status, Database, and Archive Status, configuration files and log dumps. It is further extended to set debug levels and mask sensitive information.

To start EventTracker Diagnostics Tool

- 1 Click **Start > Programs > Prism Microsystems > EventTracker > EventTracker Control Panel**

EventTracker opens **EventTracker Control Panel** window.

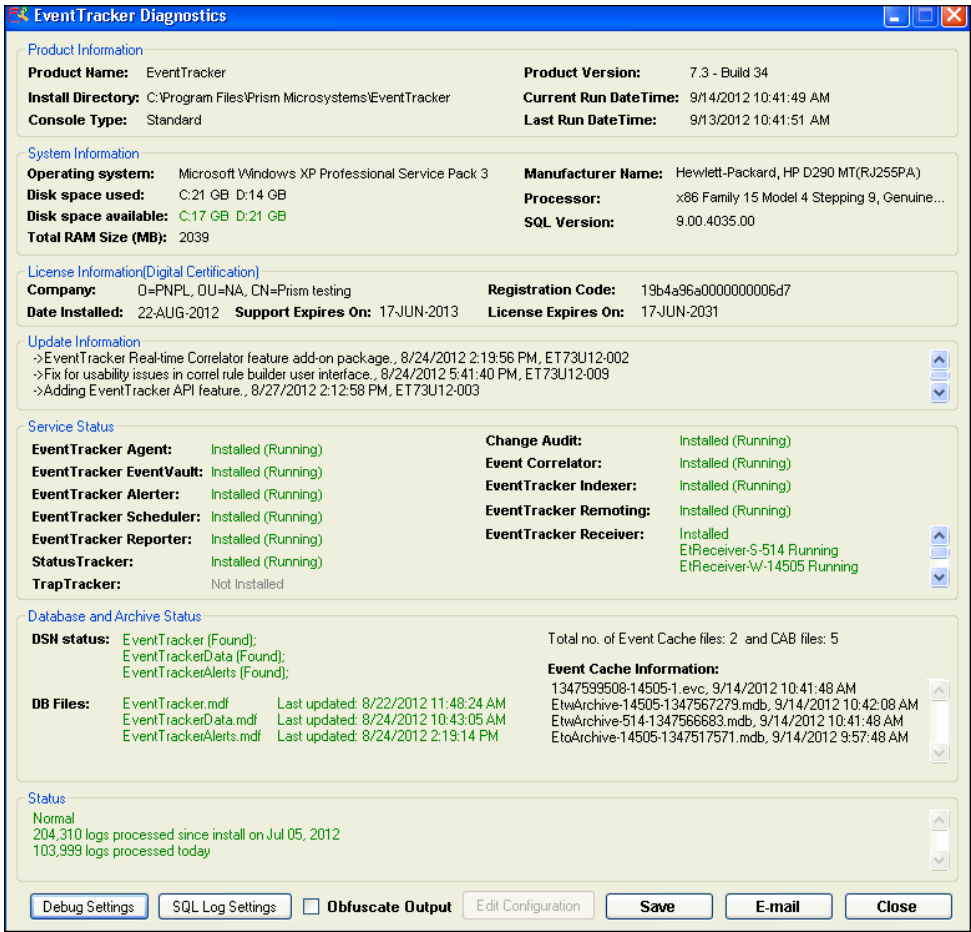
Figure 364
EventTracker
Control Panel



- 2 Click **Diagnostics** icon.

EventTracker displays **EventTracker Diagnostics** window.

Figure 365
EventTracker
Diagnostics




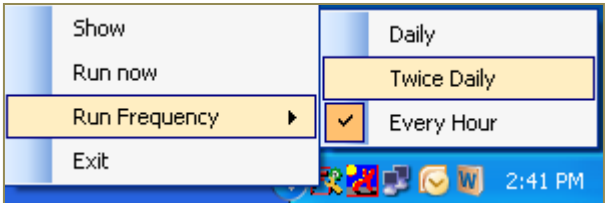
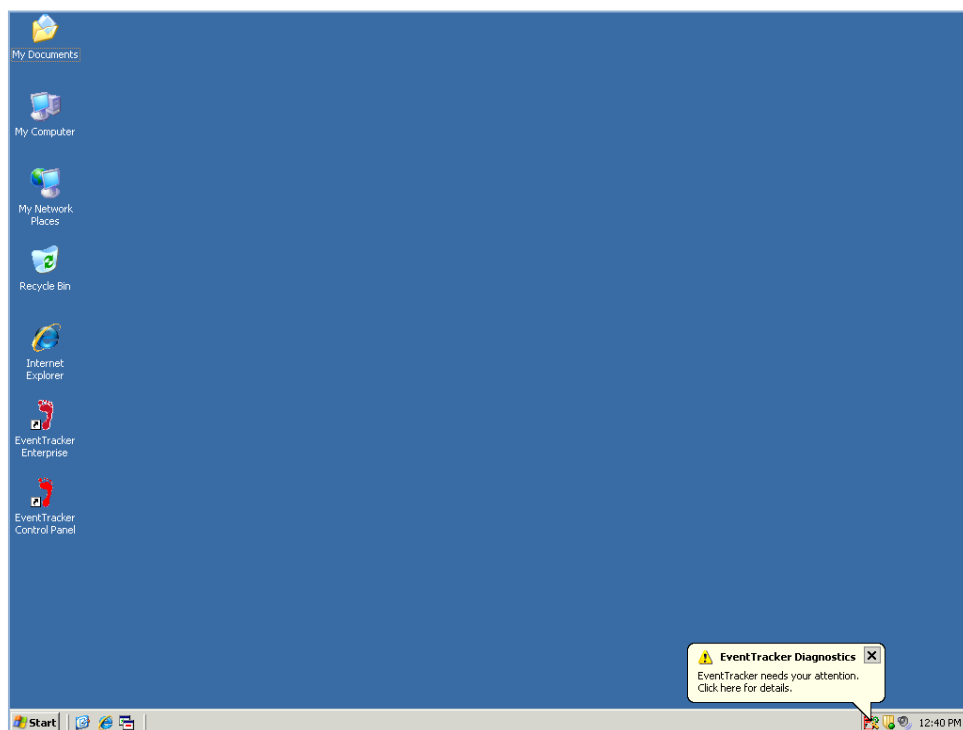
- 3 Right-click the **Diagnostics Tool** icon  on the taskbar.
EventTracker displays the shortcut menu.
- 4 To set the frequency, move the mouse pointer over the **Run Frequency** option.
EventTracker displays the options to set the frequency.

Figure 366
Diagnostics Run
frequency



If there is any error, then Diagnostics Tool displays the diagnostics message balloon to grab your attention.

Figure 367
EventTracker
Diagnostics alert



Setting Debug Levels

This option helps to set log severity levels for EventTracker modules.

To set log severity levels

- 1 Open **EventTracker Control Panel**
- 2 Click **Diagnostics**, and then click **Debug Settings** button.

Diagnostics Tool displays the Debug Levels window.

Figure 368
Debug Levels

Module	Log Level
EventTracker Web:	Warning
Receiver:	Warning
EventVault:	Critical
Scheduler:	Critical
Indexing Services:	Information
Direct Log Archiver:	Warning
Alerter:	Warning
Reporter:	Information
Enterprise Activity:	Warning
Collection Point/Master:	Not Installed
Change Audit:	Information
Correlator:	Not Installed
TrapTracker:	Warning
StatusTracker:	Not Installed

EventTracker writes the log messages in the respective log files with the severity levels set.

Table 121

EventTracker Module	Log File	Folder Path
EventTracker Web	*.*	... \Program Files\Prism Microsystems\EventTrackerWeb\Log
EventTracker Web	EventTracker.log	... \Program Files\Prism Microsystems\EventTracker\Advanced

EventTracker Module	Log File	Folder Path
		Reports\Logs
Receiver	evtrxr*.txt ex: evtrxlog-514.txt evtrxlog-14505.txt evtrxlog-14509.txt	...\Program Files\Prism Microsystems\EventTracker
EventVault	evtarlog.txt	...\Program Files\Prism Microsystems\EventTracker
Scheduler	etslog.txt	...\Program Files\Prism Microsystems\EventTracker
Indexing Services	Prism.Keyword.Indexer.*.log	...\Program Files\Prism Microsystems\EventTracker\Advanced Reports\Logs
Direct Log Archiver	LogFileParser.txt	...\Program Files\Prism Microsystems\EventTracker
Alerter	ETRSSLLog.txt	...\Program Files\Prism Microsystems\EventTracker
Reporter	Prism.EventTracker. Report*.log	...\Program Files\Prism Microsystems\EventTracker\Advanced Reports\Logs
Enterprise Activity	etuserlog.txt	...\Program Files\Prism Microsystems\EventTracker
Collection Point/Master	evtCPlog.txt	...\Program Files\Prism Microsystems\EventTracker
Change Audit	*,*	...\Program Files\Prism Microsystems\WCWindows\Logs
Correlator	etcorlog.txt	...\Program Files\Prism Microsystems\EventTracker\ETCorrel
TrapTracker	evtrxlog.txt	...\Program Files\Prism Microsystems\TrapTracker
StatusTracker	monlog.txt	...\Program Files\Prism Microsystems>StatusTracker

3 Select appropriately in the relevant fields.

4 Click **Save**.

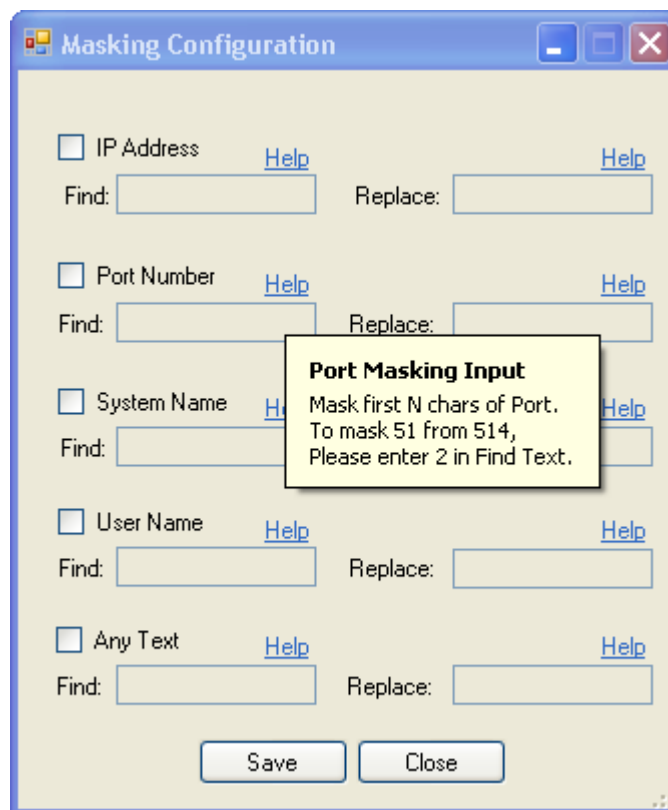
Obfuscating Classified Information

This option helps to mask classified information in log files when you send the log files outside your enterprise for debugging.

To obfuscate classified information

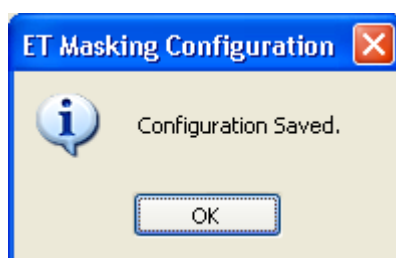
- 1 Open **EventTracker Control Panel**.
- 2 Click **Diagnostics**, and then click the **Obfuscate Output** checkbox.
Diagnostics Tool displays the **Masking Configuration** window.
- 3 Move the mouse pointer over the **Help** hyperlink to view help tips.

Figure 369
Masking
Configuration



- 4 Select the appropriate checkbox.
- 5 Click **Save** and then click the **OK** button.

Figure 370

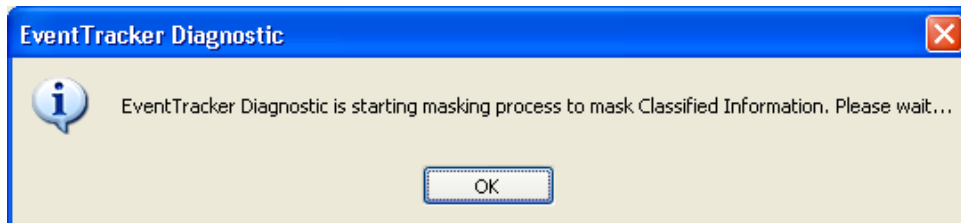


Diagnostics Tool enables the Edit Configuration button.

- 6 Click **E-mail** to send log files and configuration files for debugging.

Diagnostics Tool displays the message box indicating that the classified information being masked.

Figure 371
EventTracker
Diagnostic masking
progress



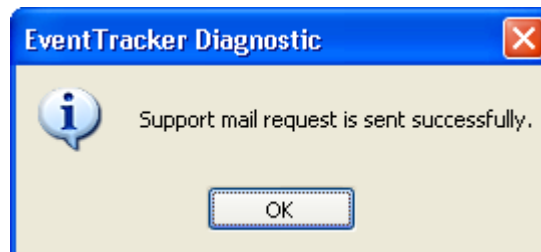
- 7 Click **OK**.

Diagnostics Tool displays the EventTracker Diagnostics window with more mailing options.

Figure 372
EventTracker
Diagnostic - Email

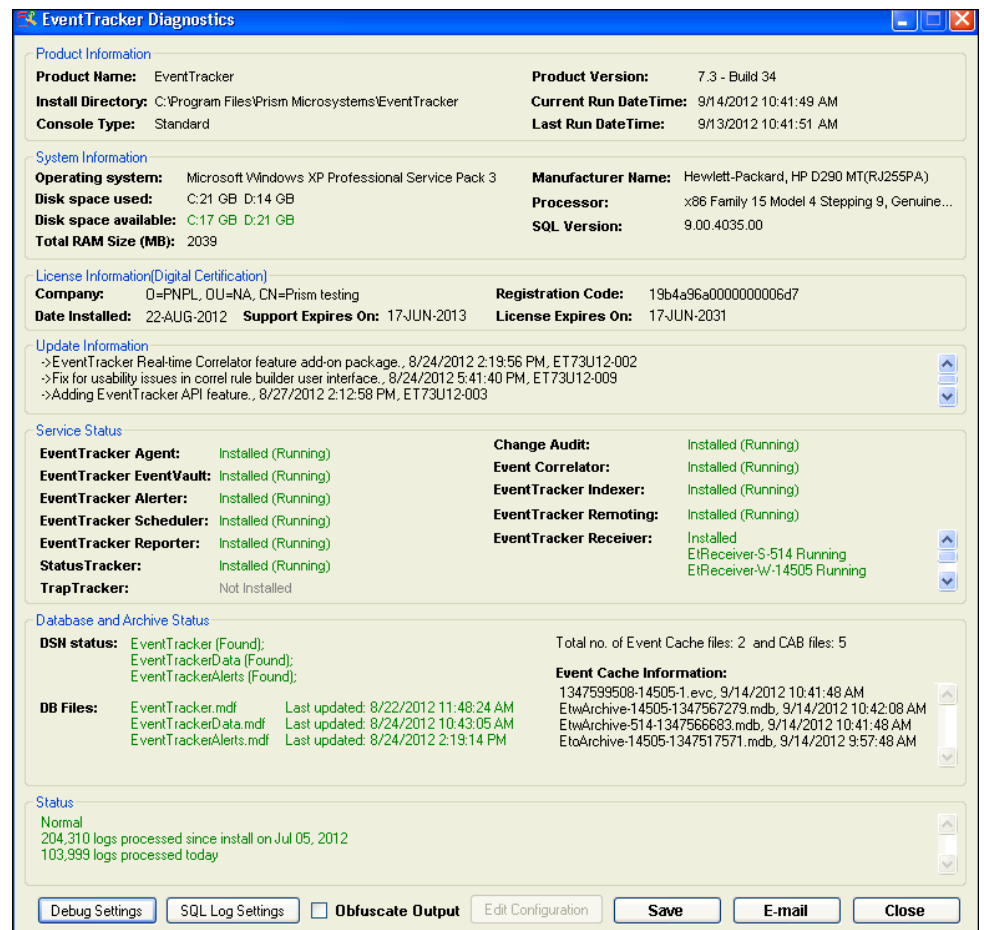
- 8 Enter/select appropriately in the relevant fields.
- 9 Click **Send**.
You will get a message in EventTracker Diagnostic pop up window saying 'Support mail request is sent successfully'.

Figure 373



You can also save the log files and configuration files as a compressed file for future reference.

- 10 Click **Save** on the EventTracker Diagnostics window.

Figure 374
EventTracker
Diagnostics

- 11 Type the problem description in the provided field.
- 12 Click **Save**.
Diagnostics Tool displays the Save As window.
- 13 Go to the appropriate folder and then click **Save**.
You can also change the name of the PIZ file.

Diagnostic Alert

When you access EventTracker from a remote location using a browser client, Diagnostics tool displays a warning message alert indicator and prompts you to respond if any problem occurs with EventTracker.

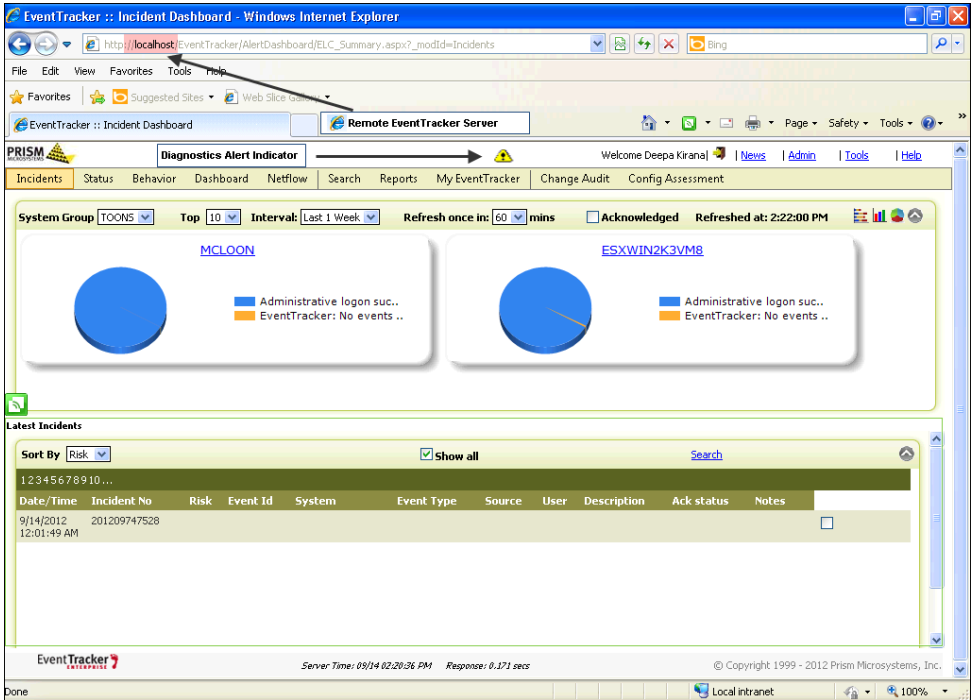
Diagnostics tool displays and hides the indicator based on the diagnostic frequency you set. By default, diagnostic frequency is set to 24 hours.

An admin user can view incident and problem descriptions. A normal user is only indicated that a problem has occurred.

- 1 Log on to EventTracker with admin user credentials.

Diagnostics tool displays the diagnostic alert indicator.

Figure 375
Diagnostic Alert




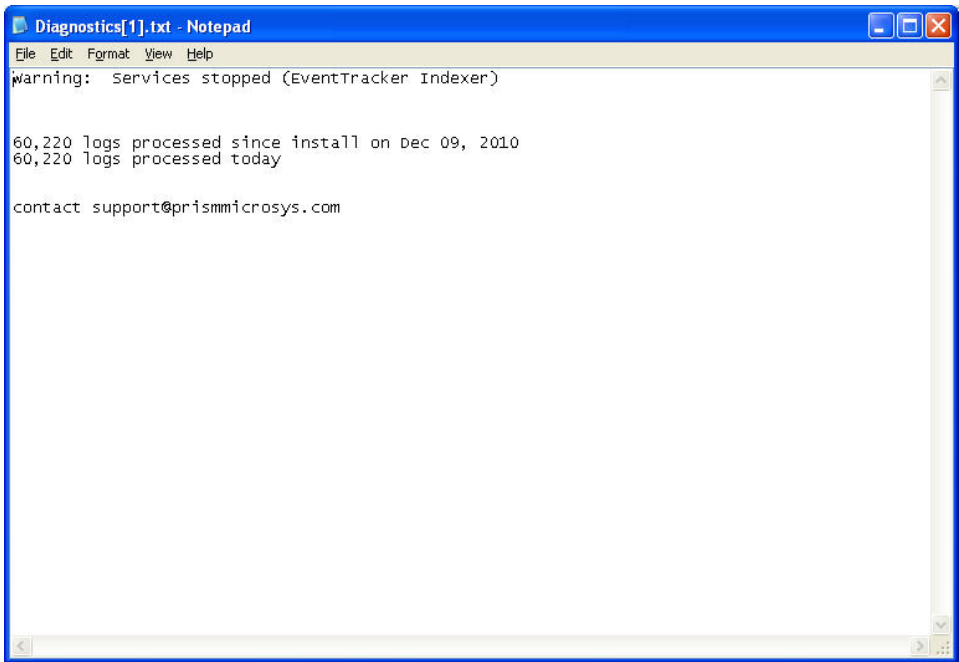
- 2 Click the indicator  icon.
EventTracker displays the File Download pop-up window to open or save the diagnostic report.
- 3 Click **O**pen to view the report.
EventTracker opens the report in the Notepad.

Figure 376
Diagnostic Report



Export and Import Utility

Export and Import Utility enables you to export/import custom Categories, Filters, Alerts, Scheduled Reports, Domains, Systems, RSS Feeds, and Behavior Rules during migrate/upgrade process, and to transfer EventTracker data from one system to the other in your enterprise. Suppose, you have configured Scheduled Reports in System A and want to configure Scheduled Reports in System B with same configuration settings. You need not configure again in System B, just export the Scheduled Reports configured in System A and then import those .issch files into System B.

Exporting Categories

To export Categories

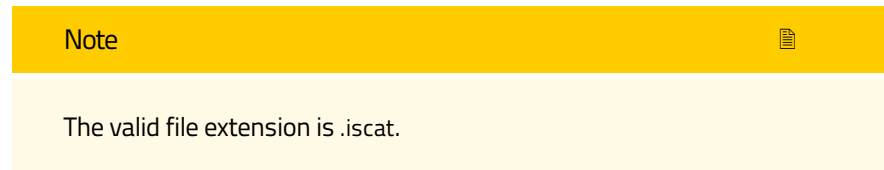
- 1 Click **Export Import Utility**.
EventTracker displays the Export Import Utility.

Table 122

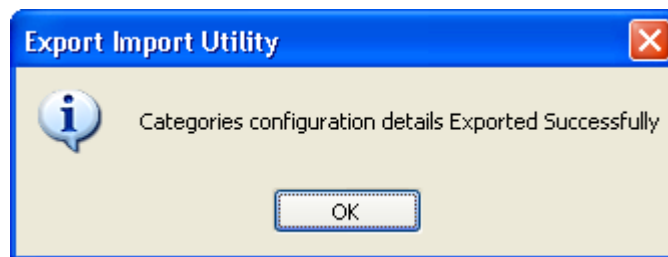
Field	Description
Category	Select a Category group(s) to add all Categories that belong to that group to the Selected list or expand the Category group(s) to add individual Category. Selected Category group(s) / Category (s) are added to the Selected list.

Field	Description
Selected	To remove Category group(s) / Category(s), clear the respective checkbox(s) in the Category list.

- Click **Export**.
EventTracker displays the Save As pop-up window.
- Type the file name in the **File name** field.



- Click **Save**.
EventTracker displays the Export Import Utility message box.



- Click **OK**.

Figure 377
Export Category -
message box

Exporting Filters

To export Filters


- Open the Export Import Utility.
- Select the **Filters** option.

Table 123

Field	Description
Filters	Select a Filter / Filters from this list. Click Add-> to add filters to the Selected list. Click Add All>> to add all Filters to the Selected list. To select multiple filters, hold down the CTRL key on your keyboard and click the filters.
Selected	Select a Filter / Filters from this list. Click <-Remove to remove the selected Filter / Filters from this list.

Field	Description
	Click <<Remove All to remove all Filters from this list.

- 3 Select the Filters and then click **Export**.
- 4 Type the file name in the **File name** field.

Note 

The valid file extension is [.isfil](#).

- 5 Click **Save**.
EventTracker displays the Export Import Utility message box.
- 6 Click **OK**.

Exporting Alerts


To export Alerts

- 1 Open the Export Import Utility.
- 2 Select the **Alerts** option.

Table 124

Field	Description
Export E-mail Settings	Select this checkbox to export Alerts along with the corresponding e-mail settings, if any.
Alerts	Select an Alert / Alerts from this list. Click Add-> to add to the Selected list. Click Add All>> to add all Alerts to the Selected list. To select multiple Alerts, hold down the CTRL key on your keyboard and click the Alerts.
Selected	Select an Alert / Alerts from this list. Click <-Remove to remove the selected Alert / Alerts from this list. Click <<Remove All to remove all Alerts from this list.

- 3 Click **Export**.
- 4 Type the file name in the **File name** field.

Note

The valid file extension is [.isalt](#).

- 5 Click **S**ave.
EventTracker displays the Export Import Utility message box.
- 6 Click **O**K.

Exporting System Groups


To export system groups

- 1 Open the Export Import Utility.
- 2 Select the **Systems and Groups** option.
EventTracker displays the systems groups.

Table 125

Field	Description
Systems and Groups	Select a system group(s) to add all systems that belong to that group to the Selected list or expand the system group(s) to add individual system. Selected system group(s) / system(s) are added to the Selected list.
Selected	To remove system group(s) / system(s), clear the respective checkbox(s) in the Systems and Groups list.

- 3 Click **E**xport.
- 4 Type the file name in the **F**ile **n**ame field.

Note

The valid file extension is [.issys](#).

- 5 Click **S**ave.
EventTracker displays the Export Import Utility message box.
- 6 Click **O**K.

Exporting Scheduled Reports


To export Scheduled Reports

- 1 Open the Export Import Utility.
- 2 Select the **Scheduled Reports** option.

Table 126

Field	Description
Scheduled Reports	<p>Select a Scheduled report / reports from this list.</p> <p>Click Add-> to add to the Selected list.</p> <p>Click Add All>> to add all Scheduled reports to the Selected list.</p> <p>To select multiple Scheduled reports, hold down the CTRL key on your keyboard and click the Scheduled reports.</p>
Selected	<p>Select a Scheduled report / reports from this list.</p> <p>Click <-Remove to remove the selected Scheduled report / reports from this list.</p> <p>Click <<Remove All to remove all Scheduled reports from this list.</p>

- 3 Click **Export**.
- 4 Type the file name in the **File name** field.

Note 

The valid file extension is [.issch](#).

- 5 Click **Save**.
EventTracker displays the Export Import Utility message box.
- 6 Click **OK**.

Exporting RSS Feeds

To export RSS Feeds


- 1 Open the Export Import Utility.
- 2 Select the **RSS Feeds** option.

Table 127

Field	Description
RSS	<p>Select a RSS Feed / RSS Feeds from this list.</p> <p>Click Add-> to add to the Selected list.</p>

Field	Description
	Click Add All>> to add all RSS Feeds to the Selected list. To select multiple RSS Feeds, hold down the CTRL key on your keyboard and click the RSS Feeds.
Selected	Select a RSS Feed / RSS Feeds from this list. Click <-Remove to remove the selected RSS Feed / RSS Feeds from this list. Click <<Remove All to remove all RSS Feeds from this list.

- Click **Export**.
- Type the file name in the **File name** field.

Note 

The valid file extension is [.issrss](#).

- Click **Save**.
EventTracker displays the Export Import Utility message box.
- Click **OK**.

Exporting Behavior Rules

To export Behavior Rules

- Open the Export Import Utility.
- Select the **Behavior Rules** option.

Table 128

Field	Description
Behavior Rules	Select a Behavior Rule / Behavior Rules from this list. Click Add-> to add to the Selected list. Click Add All>> to add all Behavior Rules to the Selected list. To select multiple Behavior Rules, hold down the CTRL key on your keyboard and click the Behavior Rules.
Selected	Select a Behavior Rule / Behavior Rules from this list. Click <-Remove to remove the selected Behavior Rule / Behavior Rules from this list. Click <<Remove All to remove all Behavior Rules from this list.

- Click **Export**.
- Type the file name in the **File name** field.

Note



The valid file extension is [.isrule](#).

- 5 Click **Save**.
EventTracker displays the Export Import Utility message box.
- 6 Click **OK**.

Importing Categories

To import Categories


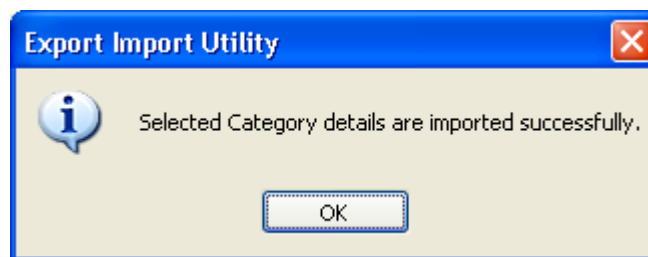
- 1 Open the Export Import Utility.
- 2 Click the **Import** tab.
EventTracker selects the **Category** option by default.
- 3 Click the browse button .
EventTracker displays the Open pop-up window.
- 4 Navigate and locate the category file you want to import.
- 5 Click **Open**.
EventTracker updates the Source field with the path of the Category file.
(OR)
Type the path of the Category file in the **Source** field.
- 6 Click **Import**.
EventTracker displays the Export Import Utility message box.


Figure 378
Import Category -
message box



- 7 Click **OK**.
-


Importing Filters

To import Filters

- 1 Open the Export Import Utility.
 - 2 Click the **Import** tab.
 - 3 Select the **Filters** option.
 - 4 Click the browse button .
EventTracker displays the Open pop-up window.
 - 5 Navigate and locate the filters file you want to import.
 - 6 Click **Open**.
EventTracker updates the **Source** field with the path of the filters file.
(OR)
Type the path of the filters file in the **Source** field.
 - 7 Click **Import**.
EventTracker displays the Export Import Utility message box.
 - 8 Click **OK**.
-

Importing Alerts

To import Alerts

- 1 Open the Export Import Utility.
- 2 Click the **Import** tab.
- 3 Select the **Alerts** option.
- 4 Click the browse button .
EventTracker displays the Open pop-up windows.
- 5 Navigate and locate the Alerts file you want to import.
- 6 Click **Open**.
EventTracker updates the Source field with the path of the Alerts file.
(OR)
Type the path of the Alerts file in the **Source** field.
By default, EventTracker selects the **Import E-mail Settings** checkbox to import Alerts along with their e-mail configuration settings.
Clear this checkbox to import Alerts without the associated e-mail settings.
- 7 Select an appropriate **Set Active** option.

Note



Active Alerts: Active Alerts are Alert events that have at least one action set.

Select the **Only if notifications set** option to make an Alert active, had you set any sort of action to the Alert.

Select the **By default** option if you wish to make an Alert active irrespective of whether the Alert has an associated action or not.

- 8 Click **Import**.

EventTracker displays the Export Import Utility message box.

- 9 Click **OK**.

Importing System Groups

To import system groups

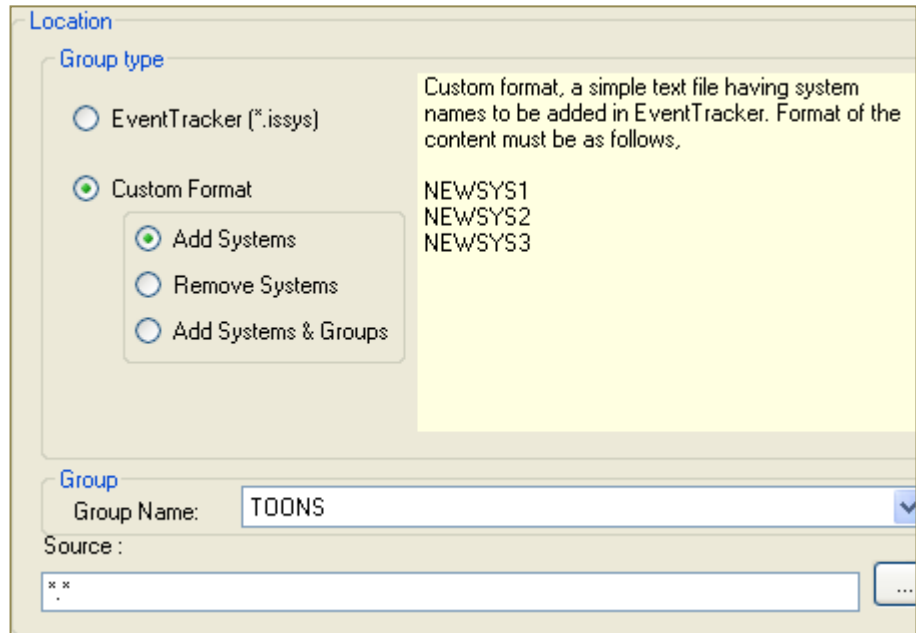
- 1 Open the Export Import Utility.
- 2 Click the **Import** tab.
- 3 Select the **Systems and Groups** option.
- 4 Select the **EventTracker (*.issys)** option to import the .issys type file.

(OR)

Select the **Custom format** option to import other type of files such as .txt files. The files should be written in the prescribed format.

- Click **Add systems** option:

Figure 379
Custom Format-
Add Systems



The screenshot shows the 'Location' dialog box with the 'Group type' section. The 'Custom Format' radio button is selected. Below it, the 'Add Systems' radio button is also selected. A text area on the right contains the following text:

```
Custom format, a simple text file having system
names to be added in EventTracker. Format of the
content must be as follows,

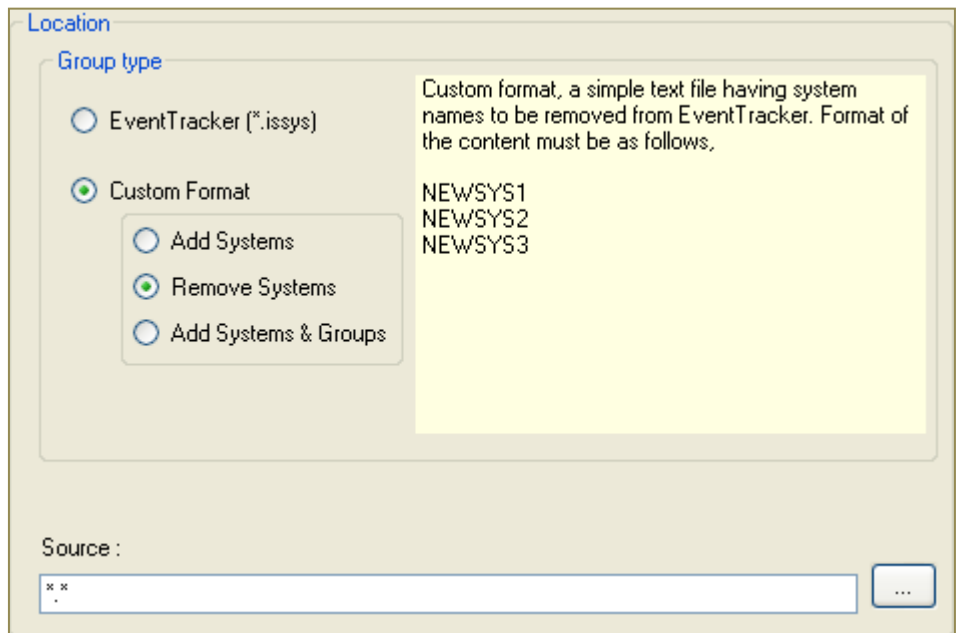
NEWSYS1
NEWSYS2
NEWSYS3
```

Below the 'Group type' section, the 'Group' section shows 'Group Name' as 'TOONS'. The 'Source' field is empty, with a placeholder 'x x' and a file selection button.

Text file contains one system name per line.

- Click **Remove systems** option:

Figure 380
Custom Format-
Remove Systems



The screenshot shows the 'Location' dialog box with the 'Group type' section. The 'Custom Format' radio button is selected. Below it, the 'Remove Systems' radio button is selected. A text area on the right contains the following text:

```
Custom format, a simple text file having system
names to be removed from EventTracker. Format of
the content must be as follows,

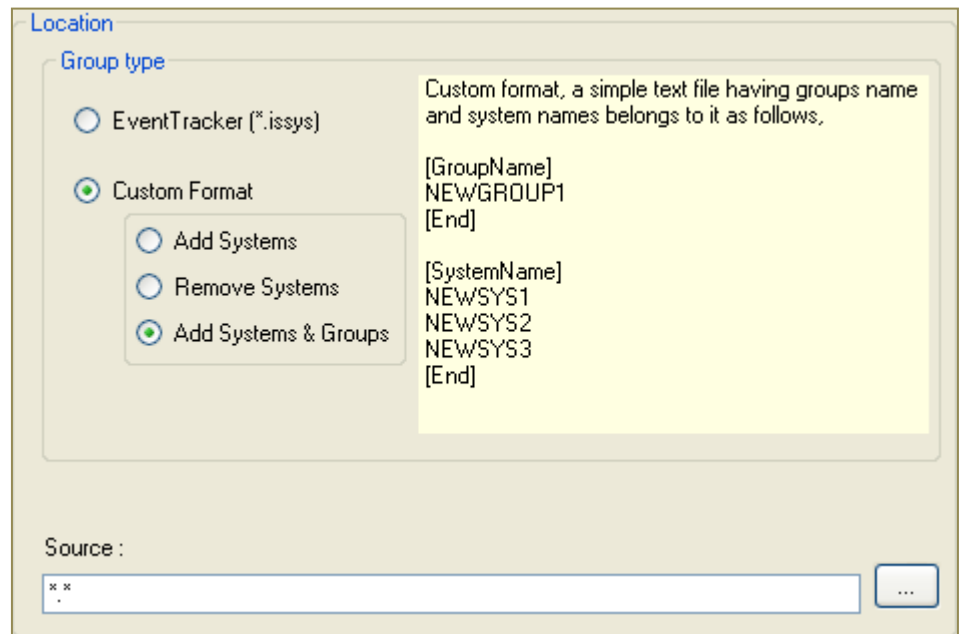
NEWSYS1
NEWSYS2
NEWSYS3
```

Below the 'Group type' section, the 'Group' section shows 'Group Name' as 'TOONS'. The 'Source' field is empty, with a placeholder 'x x' and a file selection button.

No system name included in the text file.

- Select **Add systems & Groups** option:

Figure 381
Custom Format- Add
Systems & Groups



Text file contains system and group name.

- 5 Click the browse button .

EventTracker displays the Open pop-up windows.

- 6 Navigate and locate the systems and groups file you want to import

- 7 Click **Open**.

EventTracker updates the **Source** field with the path of the systems and groups file.

(OR)

Type the path of the systems and groups file in the **Source** field.


- 8 Click **Import**.

EventTracker displays the Export Import Utility message box.

- 9 Click **OK**.

Importing Scheduled Reports

To import Schedule Reports

- 1 Open the Export Import Utility.
- 2 Click the **Import** tab.
- 3 Select the **Scheduled Reports** option.
- 4 Click the browse button .

EventTracker displays the Open pop-up window.

5 Navigate and locate the Scheduled reports file you want to import.

6 Click **Open**.

EventTracker updates the **Source** field with the path of the Scheduled reports file.

(OR)

Type the path of the Scheduled reports file in the **Source** field.

7 Click **Import**.

EventTracker displays the Export Import Utility message box.

8 Click **OK**.

Importing RSS Feeds

To import RSS Feeds

1 Open the Export Import Utility.

2 Click the **Import** tab.

3 Select the **RSS** option.

4 Click the browse button .

EventTracker displays the Open pop-up window.

5 Navigate and locate the scheduled reports file you want to import.

6 Click **Open**.

EventTracker updates the Source field with the path of the RSS Feeds file.

(OR)

Type the path of the RSS Feeds file in the **Source** field.

7 Click **Import**.

EventTracker displays the Export Import Utility message box.

8 Click **OK**.

Importing Behavior Rules

To import Behavior Rules

1 Open the Export Import Utility.

2 Click the **Import** tab.

3 Select the **Behavior Rules** option.

4 Click the browse button .

EventTracker displays the Open pop-up window.

5 Navigate and locate the Behavior Rules file you want to import.

6 Click **Open**.

EventTracker updates the Source field with the path of the Behavior Rules file.

(OR)

Type the path of the Behavior Rules file in the **Source** field.

7 Click **Import**.

EventTracker displays the Export Import Utility message box.

8 Click **OK**.

Importing SCAP Content

To import SCAP Content

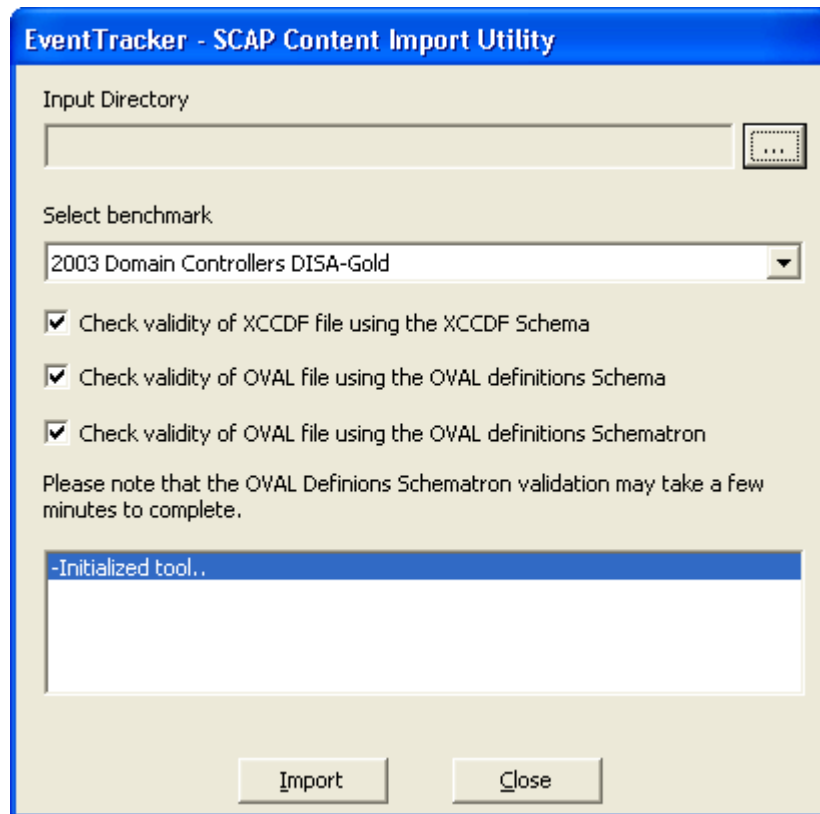
1 Open the Export Import Utility.

2 Click the **Import** tab.

3 Select the **SCAP** option.

EventTracker displays the **EventTracker - SCAP Content Import Utility** pop-up window.

Figure 382
SCAP Content
Import Utility



All the 'Check validity...' checkboxes are selected by default.

- 4 Click the browse button .

EventTracker displays the **Browse for folder** pop-up window.

- 5 Navigate and locate the input directory that contains SCAP content XML files.
- 6 Click **Ok**.
- 7 Select appropriate benchmark from the **Select benchmark** dropdown.
EventTracker displays the Export Import Utility message box.
- 8 Click **OK**.

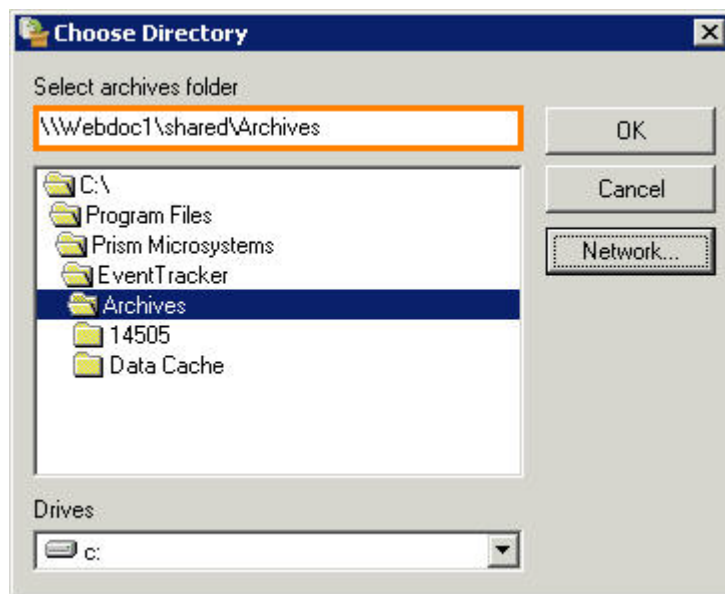
Appending CAB Files

Append Archiver appends CAB files to the Archives folder and updates the archive index with minimal time consumption.

To append CAB files

- 1 Double-click **Append Archives** on the EventTracker Control Panel.

Figure 384
Choose Directory
window



- 3 Click **OK**.

EventVault Warehouse Manager displays the Append Archives window with CAB files to append.




















Figure 385
Append Archives
window



Append Archives

Source archives path
\\Webdoc1\shared\Archives

☒ Search in Sub Folders

Destination: C:\Program Files\Prism Microsystems\EventTracker\Archives

	Cab Name	Cab Path
<input type="checkbox"/> 	etar1273814383-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1273861816-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1273948232-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1273948236-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274034649-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274034667-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274121037-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274121046-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274243469-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274368559-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274368576-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274511982-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274512014-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274662217-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274662237-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274701818-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274701848-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274701854-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/> 	etar1274701860-14505.cab	\\webdoc1\shared\Archives\14505\2010\5

☐ Select all missing files  Cab Present  Cab Missing

OK Cancel

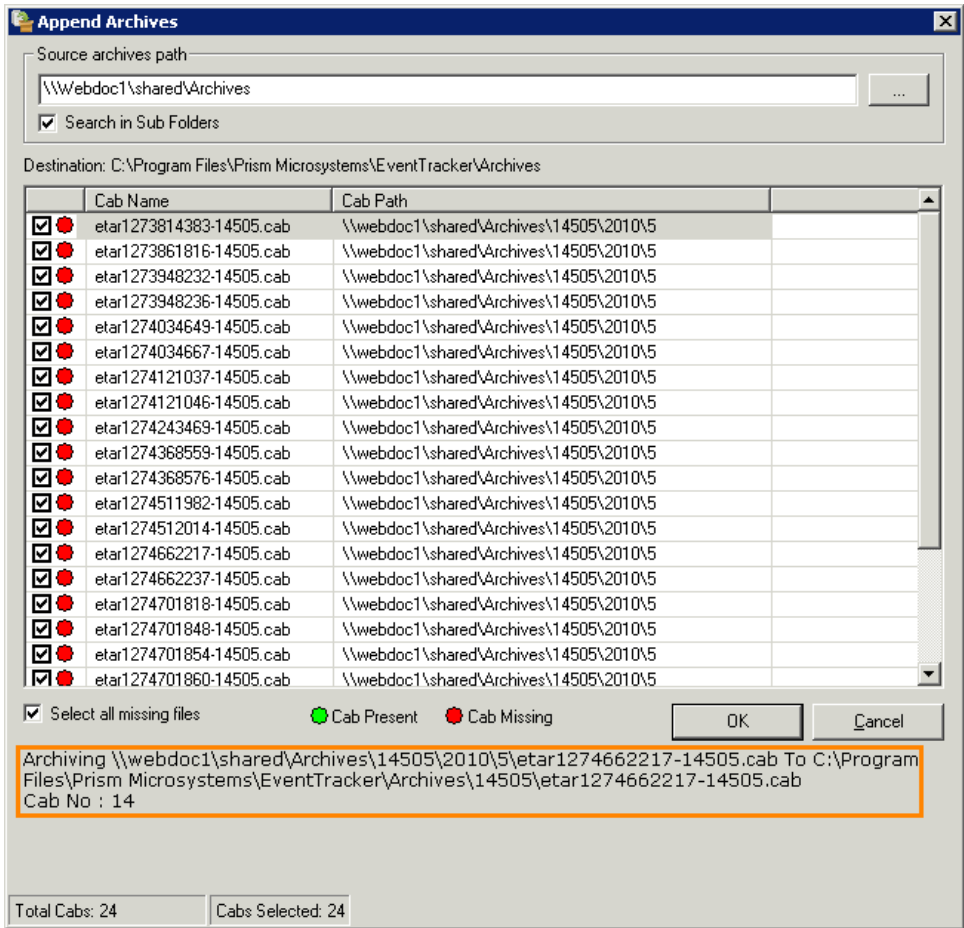
Total Cabs: 24 Cabs Selected: 0

You can select individual files by selecting the checkboxes against the respective CAB files or collectively by selecting the **Select all missing cabs** checkbox.

4 Click **OK**.

EventVault Warehouse Manager displays the progress of appending process.

Figure 386
Append Archives
window



After the successful completion, EventVault Warehouse Manager displays the Append Archives message box.

Figure 387
Append Archive
message box



- 5 Click **OK**.
EventVault Warehouse Manager displays the Append Archives window with list of CAB files appended.

Figure 388
Append Archives
window

Append Archives

Source archives path:
\\Webdoc1\shared\Archives

☒ Search in Sub Folders

Destination: C:\Program Files\Prism Microsystems\EventTracker\Archives

	Cab Name	Cab Path
<input type="checkbox"/>	etar1273814383-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input checked="" type="checkbox"/>	etar1273861816-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1273948232-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1273948236-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274034649-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input checked="" type="checkbox"/>	etar1274034667-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274121037-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274121046-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274243469-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input checked="" type="checkbox"/>	etar1274368559-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274368576-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274511982-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274512014-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274662217-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input checked="" type="checkbox"/>	etar1274662237-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274701818-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274701848-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input type="checkbox"/>	etar1274701854-14505.cab	\\webdoc1\shared\Archives\14505\2010\5
<input checked="" type="checkbox"/>	etar1274701860-14505.cab	\\webdoc1\shared\Archives\14505\2010\5

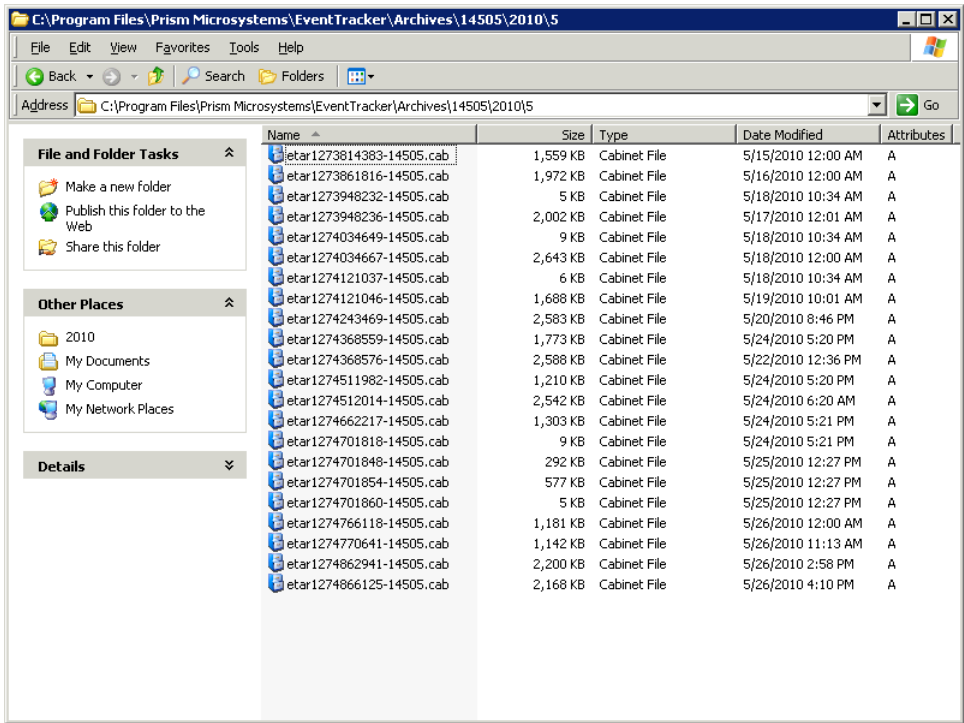
☒ Select all missing files ● Cab Present ● Cab Missing

OK Cancel

Total Cabs: 24 Cabs Selected: 24

EventVault Warehouse Manager appends the cab files to the appropriate folders.

Figure 389
Appended Archives



Event Traffic Analysis

After EventTracker is deployed on numerous systems in a large Network it is very likely that you notice EventTracker receiving millions of events. Actually a majority of these events would be of little use to you. Using appropriate priority you can filter out unnecessary events to improve utility. 'Filtering unnecessary events' is a powerful feature based on priority configured by you.

Traffic Analyzer is a tool that is part of the EventTracker. It helps to find the details of the most common events and to set your order of priority. Accordingly create filters for non-essential events that are just increasing traffic but have little value.

Filtering is a continuous process. Priority may vary from one system to another. Over a period of time, with your experience, priority events can be separated from non-priority events in a specific system. Repeating this process every week enables you to receive only events of value in optimizing your operations. When non-priority events are filtered out EventTracker functions optimally.

This report provides total counts per system for each event id. Filter and display event count details based on user-defined criteria.

Usage: Analyze Windows specific security events, correlate events, broad searches per criteria with subsequent sorting and ordering of the result set.

To start Traffic Analyzer

- Double-click **Traffic Analyzer** on the EventTracker Control Panel.
EventTracker displays the Traffic Analyzer.

Figure 390
Traffic Analyzer

Traffic Analysis – View by Category

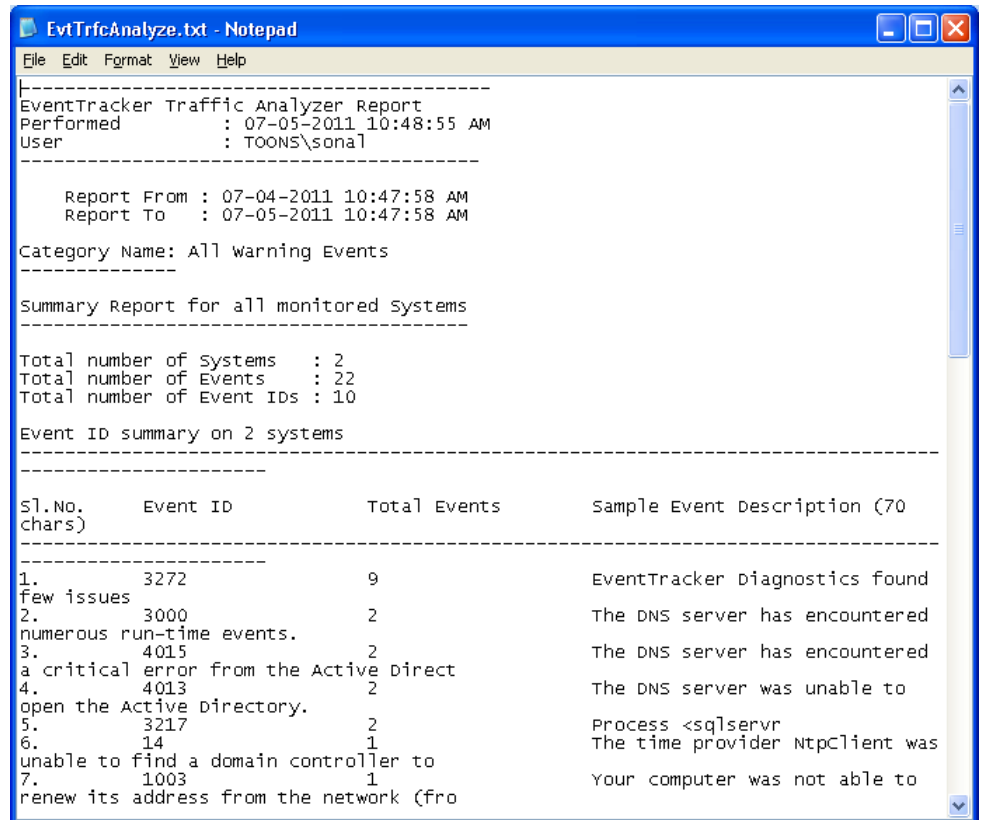
This option helps you analyze events based on Category.

To analyze event traffic – View by Category

- 1 Select the **View by Category** option, if not selected.
- 2 Select a Category from the **Category** drop-down list. Example: All Warning Events.
- 3 Set the From, To date and time range through the **From**, **To** spin boxes.

- 4 Select the **All Systems** option to select all monitored systems.
(OR)
Select the **Specific Systems** option.
Type the name of the systems separated by comma in the text box provided.
- 5 Click **Analyze**.
Traffic Analyzer displays the report in the Notepad.

Figure 391
EvtTrfcAnalyze



```

EvtTrfcAnalyze.txt - Notepad
File Edit Format View Help
-----
EventTracker Traffic Analyzer Report
Performed      : 07-05-2011 10:48:55 AM
User          : TOONS\sonal
-----
Report From   : 07-04-2011 10:47:58 AM
Report To    : 07-05-2011 10:47:58 AM
Category Name: All Warning Events
-----
Summary Report for all monitored Systems
-----
Total number of Systems   : 2
Total number of Events    : 22
Total number of Event IDs : 10
Event ID summary on 2 systems
-----
S1.No.      Event ID      Total Events      Sample Event Description (70
chars)
-----
1.          3272          9                EventTracker Diagnostics found
few issues
2.          3000          2                The DNS server has encountered
numerous run-time events.
3.          4015          2                The DNS server has encountered
a critical error from the Active Direct
4.          4013          2                The DNS server was unable to
open the Active Directory.
5.          3217          2                Process <sqlservr
6.          14           1                The time provider Ntpclient was
unable to find a domain controller to
7.          1003          1                Your computer was not able to
renew its address from the network (fro

```

Correlating Events

This option enables you to correlate events with the offline events in the database.

To correlate events

- 1 Select the **All Correlation Events** option from the Category drop-down list.
- 2 Set the From, To date and time range through the **From, To** spin boxes.
- 3 Select the **All Systems** option to select all monitored systems.
(OR)
Select the **Specific Systems** option.

Type the name of the systems separated by comma in the text box provided.

4 Click **Analyze**.

Traffic Analyzer displays the Flex Report report EvtTrfcAnalyze in the Notepad.

Traffic Analysis – View by Event Id

This option helps you analyze hard coded Windows specific security events.

To analyze event traffic – View by Event Id

- 1 Select the **View by Event Id** option.

Figure 392
Traffic Analyzer

Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria

☐ View by Category ☒ View by Event Id ☐ View by Custom Selection ☐ Keywords Analysis

Analysis of specific Windows events.

☒ Display all records ☐ Display only top 10 records

Select Event Id

<input type="checkbox"/>	[540,4624] Successful Network Logon
<input type="checkbox"/>	[672,4768,4772] Authentication Ticket Granted
<input type="checkbox"/>	[673,4769,4773] Service Ticket Granted
<input type="checkbox"/>	[675,4771] Pre-authentication failed
<input type="checkbox"/>	[680,4776] Logon attempt

Select Time Range

From: 9 /13/2012 4 :57:59 PM

To: 9 /14/2012 4 :57:59 PM

Select Systems

☒ All Systems ☐ Specific Systems

Events Transfer Mode

☒ Real time ☐ Non Real time

Analyze Close

Table 129

Field	Description
Display all records:	By default, this option is selected. All records will be displayed in the report in descending order.
Display only top:	You can select this option if you want only a specified number of records to be displayed in the report.

Select Event Id: You can select 5 hard coded Windows security events for event traffic analysis.	
540 Successful Network Logon	Selecting this id will generate 2 reports sorted by Username and IP address .
672 Authentication Ticket Granted	Selecting this id will generate 2 reports sorted by Username and IP address .
673 Service Ticket Granted	Selecting this id will generate 1 report sorted by IP Address .
675 Pre-authentication failed	Selecting this id will generate 2 reports sorted by Username and IP address .
680 Logon attempt	Selecting this id will generate 2 reports sorted by Username and Computer .

- 2 Type / select appropriately in the relevant fields.
- 3 Select the **All Systems** option to select all monitored systems.
(OR)
Select the **Specific Systems** option.
Type the name of the systems separated by comma in the text box provided.
- 4 Click **Analyze**.
Traffic Analyzer displays the report in the Notepad.
If you wish to display only a specified number of records in the report, type the number of records in the **Display only top** field or click the spin box.

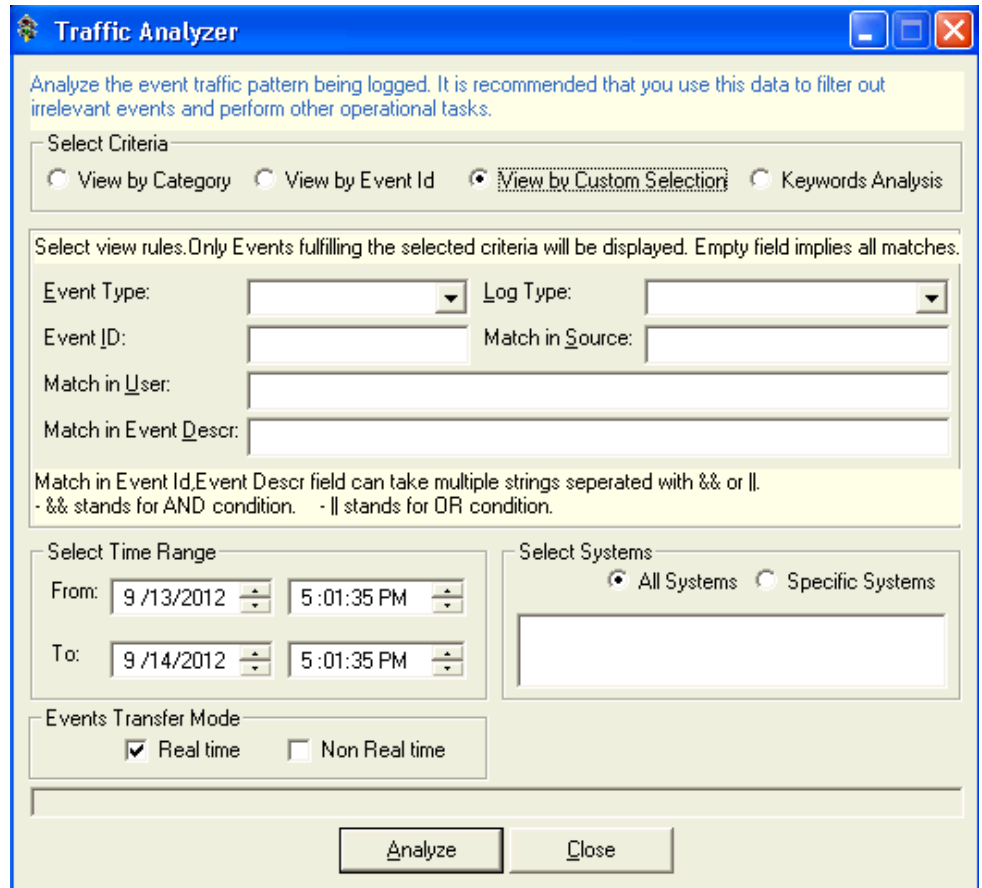
Traffic Analysis – View by Custom Selection

This option helps you customize the selection criteria.

To analyze event traffic – View by Custom Selection

- 1 Select the **View by Custom Selection** option.

Figure 393
Traffic Analyzer



- 2 Type appropriately in the relevant fields.
- 3 Select the **All Systems** option to select all monitored systems.
(OR)
Select the **Specific Systems** option.
Type the name of the systems separated by comma in the text box provided.
- 4 Click **Analyze**.
Traffic Analyzer displays the report in the Notepad.

Traffic Analysis – Keyword Analysis

This option helps to analyze traffic by keywords.

To analyze event traffic – by keywords

- 1 Select the **Keywords Flex Report** option.

Figure 394
Traffic Analyzer

Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria

☐ View by Category ☐ View by Event Id ☐ View by Custom Selection ☒ Keywords Analysis

Keywords Analysis

Contains: ☒ All ☐ Specific words

☒ Exclude following words

Add

Edit

Remove

and
for
in
is
of
or
to
was

Add

Edit

Remove

Select Time Range

From: 9 /14/2012 4 :04:17 PM

To: 9 /14/2012 5 :04:17 PM

Select Systems

☒ All Systems ☐ Specific Systems

Events Transfer Mode

☒ Real time ☐ Non Real time

Analyze

Close

Table 130

Field	Description
Keywords Analysis: Helps to analyze events by keywords.	
Contains All	Analyze logs that contain all keywords.
Contains Specific words	Analyze logs that contain specific keywords.
Excluding following words	Select this checkbox to exclude commonly occurring words.

2 Type appropriately in the relevant fields.

3 Select the **All Systems** option to select all monitored systems.
(OR)
Select the **Specific Systems** option.
Type the name of the systems separated by comma in the text box provided.

4 Click **Analyze**.
EventTracker displays the report in the Notepad.

EVENTTRACKER DIAGNOSTIC TOOL

505

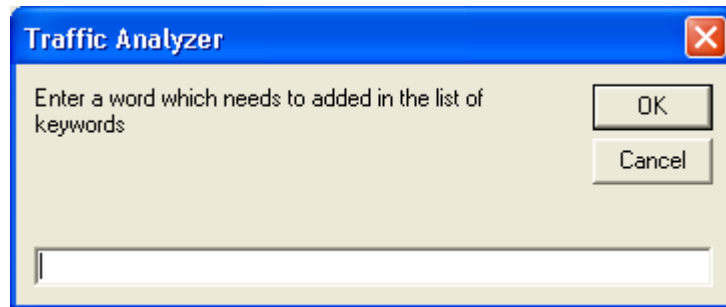
Adding Keywords for Analysis

This option helps to add keywords.

To add keywords

- 1 Select the **Specific words** option.
Traffic Analyzer enables the Add, Edit, and Remove buttons.
- 2 Click **Add**.
Traffic Analyzer displays the Traffic Analyzer dialog box.

Figure 395
Traffic Analyzer



- 3 Type the keyword in the text box provided. Example: ETAdmin
- 4 Click **OK**.
Traffic Analyzer adds the keyword to the list of keywords.

Figure 396
Traffic Analyzer

Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria

☐ View by Category ☐ View by Event Id ☐ View by Custom Selection ☒ Keywords Analysis

Keywords Analysis

Contains: ☒ All ☐ Specific words ☐ Exclude following words

and
for
in
is
of
or
to
was

Select Time Range

From: 9/14/2012 4:04:17 PM

To: 9/14/2012 5:04:17 PM

Select Systems

☒ All Systems ☐ Specific Systems

Events Transfer Mode

☒ Real time ☐ Non Real time

- 5 To analyze logs that contain a specific keyword, select a keyword from the list and then click **Analyze**.

Adding Commonly Occurring Words to Exclude from Analysis

This option helps to add most commonly occurring words to exclude from analysis.

To add words to exclude from analysis

- 1 Select the **Exclude following words** checkbox.

Traffic Analyzer displays the list of commonly occurring words, enables Add, Edit, and Remote buttons.

Figure 397
Traffic Analyzer

- 2 Click **Add**.

Traffic Analyzer displays the Traffic Analyzer dialog box.

Figure 398
Traffic Analyzer

- 3 Type the keyword in the text box provided.
- 4 Click **OK**.

Traffic Analyzer adds the new keyword to the list for exclusion.

Windows Agent Management Tool

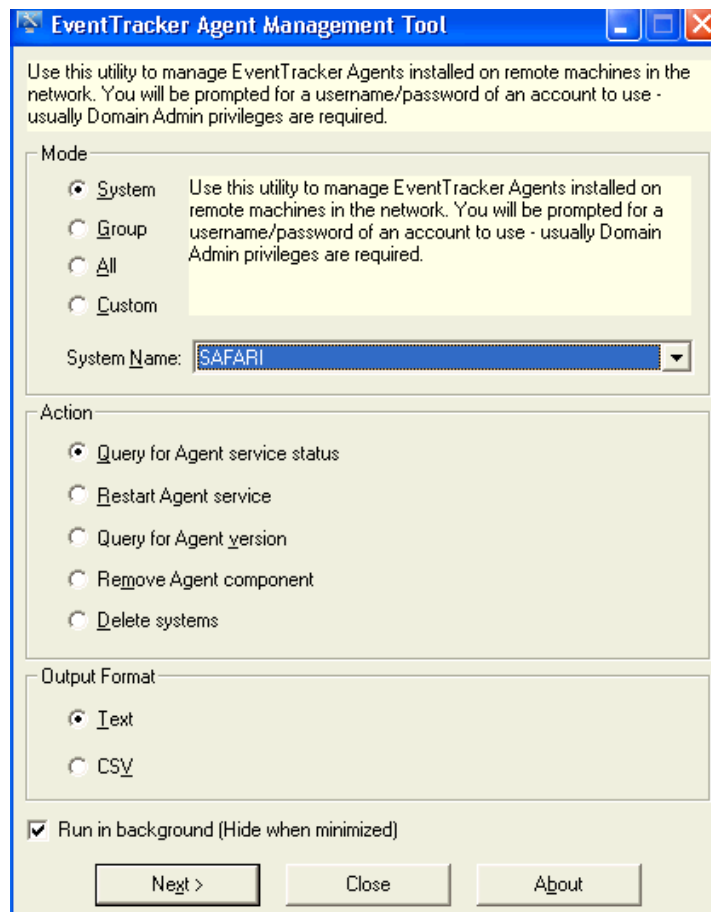
Agent Management Tool is a diagnostic tool to check the health status of remote agents, restart the failed agent services and to check the version of remote agents. You ought to have Domain Admin privilege to use this utility.

Accessing Agent Management Tool

To access the Agent Management Tool

- Double-click **Agent Management Tool** on the EventTracker Control Panel.
EventTracker displays the Agent Management Tool.

Figure 399
Agent Management
Tool



Querying Agent Service Status - System

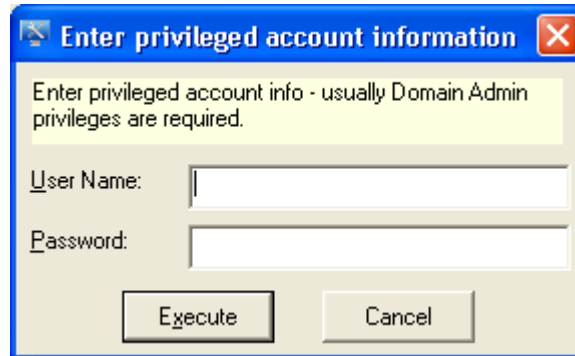
This option enables you to query agent service status in the selected system.

To query agent service status in the selected system

- 1 Select the **System** option, if not selected.
- 2 Select the system from the **System Name** drop-down list.
- 3 Select the **Query for Agent service status** option, if not selected.
- 4 Click **Next >**.

EventTracker displays the Enter Privileged account information dialog box.

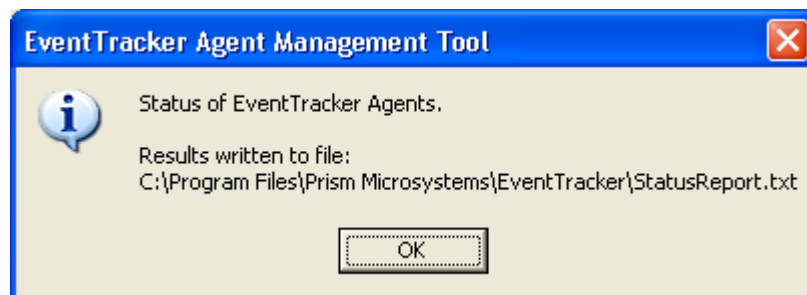
Figure 400
Enter privileged
account information



- 5 Type valid user name and password respectively in the **User Name** **Password** fields.
- 6 Click **Execute**.

EventTracker displays the EventTracker Management Tool message box.

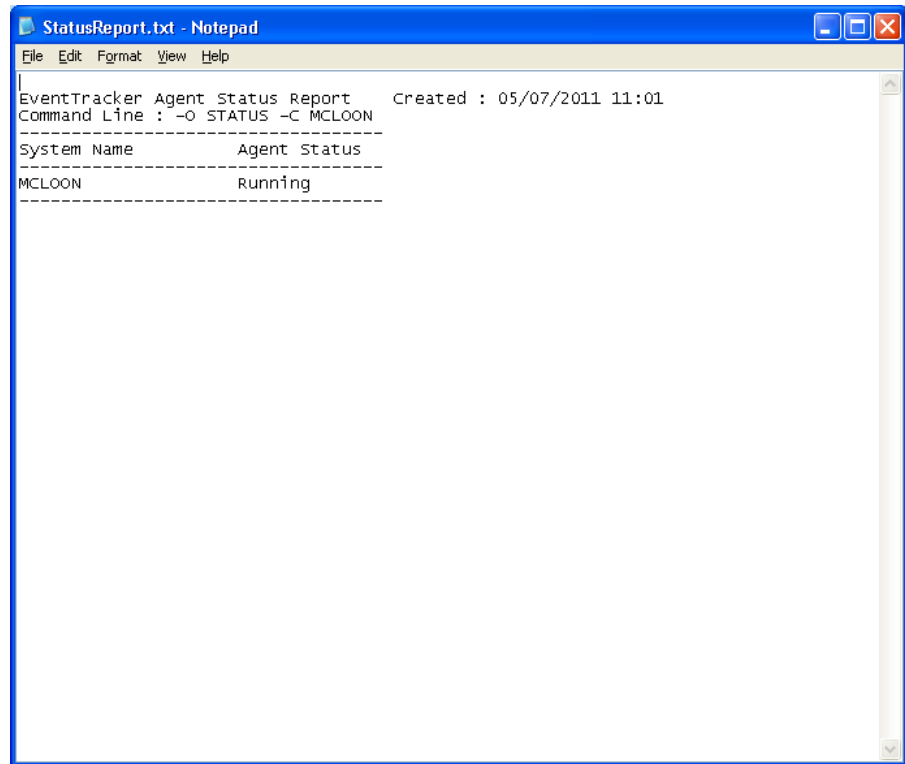
Figure 401
EventTracker
Management Tool
message box



- 7 Click **OK**.

EventTracker displays the result in the Notepad.

Figure 402
EventTracker
Management Tool -
Status Report



Querying Agent Service Status - Group

This option enables you to query status of the agent service in the selected group.

To query agent service status in the selected group

- 1 Select the **Group** option.
 - 2 Select the Group from the **Group Name** drop-down list.
 - 3 Select the **Query for Agent service status** option, if not selected.
 - 4 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 5 Type valid username and password and then click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 6 Click **OK**.
EventTracker displays the result in the Notepad.
-

Querying Agent Service Status - All

This option enables you to query the agent service status running in all systems and system groups.

To query agent service status in all systems and system groups

- 1 Select the **All** option.
 - 2 Select the **Query for Agent service status** option.
 - 3 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 4 Type valid username and password and then click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 5 Click **OK**.
EventTracker displays the result in the Notepad.
-

Querying Agent Service Status – Custom

This option is provided you to query the agent service status for specified systems. This option enables you to focus on the specific systems listed in the text file. The text file contains system names (one system per line).

To query agent service status in all systems and system groups


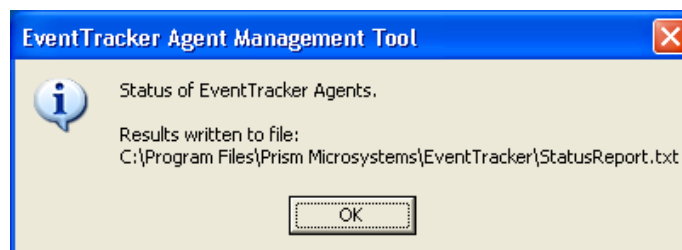
- 1 Select the **Custom** option.
- 2 Click the  button and select the text file containing system names.
- 3 Click **Open**.
- 4 Select the **Query for Agent service status** option.
- 5 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
- 6 Type valid username and password and then click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.

Figure 403



- 7 Click **OK**.
EventTracker displays the result in the Notepad.

Restarting Agent Service - System

This option enables you to restart the agent service in the selected system.

To restart the agent service in the selected system

- 1 Select the **S**ystem option.
- 2 Select the system from the **System Name** drop-down list.
- 3 Select the **R**estart Agent service option.
- 4 Click **N**ext >.
EventTracker displays the Enter privileged account information dialog box.
- 5 Type valid username and password.
- 6 Click **E**xecute.
EventTracker displays the EventTracker Agent Management Tool message box.
- 7 Click **O**K.
EventTracker displays the result in the Notepad.

Restarting Agent Service - Group

This option enables you to restart the agent service in the selected group.

To restart the agent service in the selected group

- 1 Select the **G**roup option.
- 2 Select the Group from the **Group Name** drop-down list.
- 3 Select the **R**estart Agent service option.
- 4 Click **N**ext >.
EventTracker displays the 'Enter privileged account information' dialog box.
- 5 Type valid username and password.
- 6 Click **E**xecute.
EventTracker displays the EventTracker Agent Management Tool message box.
- 7 Click **O**K.
EventTracker displays the result in the Notepad.

Restarting Agent Service - All

This option enables you to restart the agent service in all systems and system groups.


To restart the agent service in all the systems and the groups

- 1 Select the **All** option.
 - 2 Select the **Restart Agent service** option.
 - 3 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 4 Type valid username and password.
 - 5 Click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 6 Click **OK**.
EventTracker displays the result in the Notepad.
-

Restarting Agent Service - Custom

This option enables you to restart the agent service for all the systems listed in the text file.

To restart the agent service in all the systems and the groups

- 1 Select the **Custom** option.
 - 2 Click the  button and select the text file containing system names.
 - 3 Click **Open**.
 - 4 Select the **Restart Agent service** option.
 - 5 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 6 Type valid username and password.
 - 7 Click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 8 Click **OK**.
EventTracker displays the result in the Notepad.
-

Querying Version of the Agent Service - System

This option enables you to query the version of the agent service in the selected system.

To query the version of the agent service in the selected system

- 1 Select the **S**ystem option.
 - 2 Select the system from the **System Name** drop-down list.
 - 3 Select the **Query for Agent version** option.
 - 4 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 5 Enter valid username and password.
 - 6 Click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 7 Click **OK**.
EventTracker displays the result in the Notepad.
-

Querying Version of the Agent Service - Group

This option enables you to query the version of the agent service in the selected group.

To query the version of the agent service in the selected group

- 1 Select the **G**roup option.
 - 2 Select the Group from the **Group Name** drop-down list.
 - 3 Select the **Query for Agent version** option.
 - 4 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 5 Type valid username and password.
 - 6 Click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 7 Click **OK**.
EventTracker displays the result in the Notepad.
-

Querying Version of the Agent Service - All

This option enables you to query the version of the agent service in all systems and groups.


To query the version of the agent service in all the systems and groups

- 1 Select the **All** option.
 - 2 Select the **Query for Agent version** option.
 - 3 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 4 Type valid username and password.
 - 5 Click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 6 Click **OK**.
EventTracker displays the result in the Notepad.
 - 7 Click **Close** to close the EventTracker Agent Management Tool.
-

Querying Version of the Agent Service - Custom

This option enables you query the version of the agent service for all the systems listed in the text file.

To restart the agent service in all the systems and the groups

- 1 Select the **Custom** option.
 - 2 Click the  button and select the text file containing system names.
 - 3 Click **Open**.
 - 4 Select the **Query for Agent version** option.
 - 5 Click **Next >**.
EventTracker displays the Enter privileged account information dialog box.
 - 6 Type valid username and password.
 - 7 Click **Execute**.
EventTracker displays the EventTracker Agent Management Tool message box.
 - 8 Click **OK**.
EventTracker displays the result in the Notepad.
-

Removing the Agent Component

This option enables you remove the version of the agent service for all the systems listed in the text file.

- 1 Select the Remove agent component option
- 2 EventTracker displays **EventTracker Agent Management Tool** popup
- 3 Click **OK**.
- 4 Selected system name from the drop down will be removed.

Deleting Systems from the agent service

- 1 This option enables you delete the version of the agent service for all the systems listed in the text file.
- 2 Select delete systems and click next
- 3 EventTracker displays EventTracker management tool pop up
- 4 Click **OK**
- 5 Selected system name will be deleted

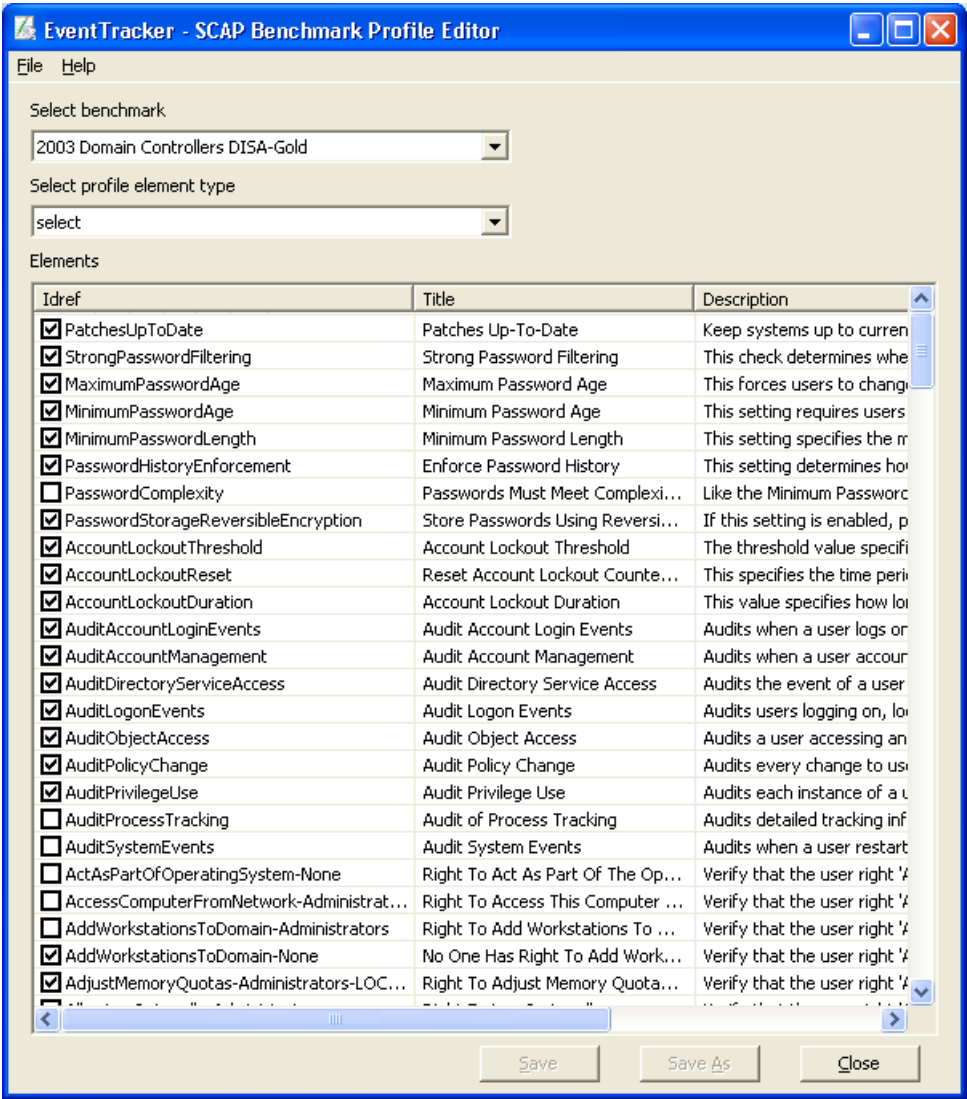
SCAP Benchmark Profile Editor

This option helps you to tailor/edit the predefined SCAP benchmark profile. You can save the updated benchmark profile as a new profile with different name.

-
- 1 Double-click **SCAP Profile Editor** on the EventTracker Control Panel.

EventTracker displays SCAP Benchmark profile editor pop-up window.

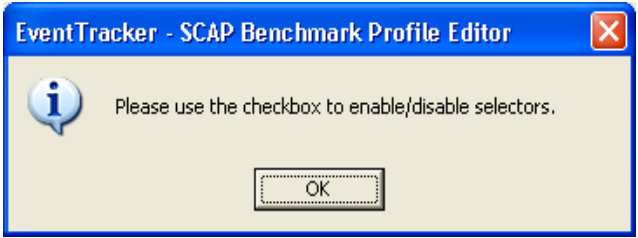
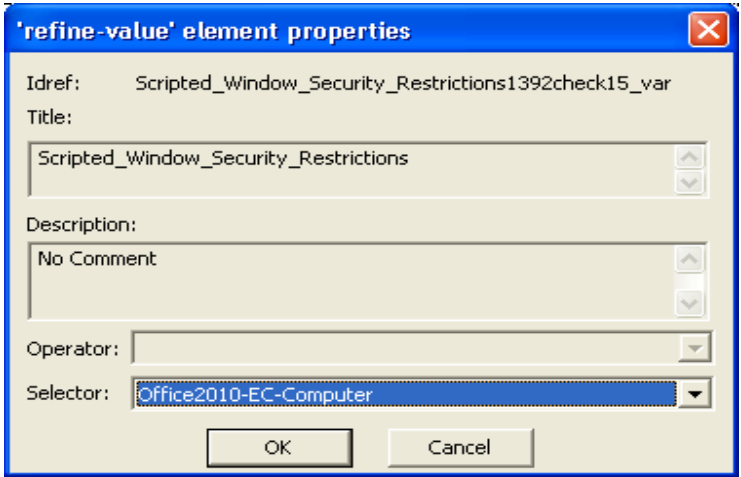
Figure 404
SCAP benchmark
profile Editor



- 2 In the **Select benchmark** dropdown, select an installed benchmark you wish to edit.
- 3 Select the type of profile element from **Select profile element type** dropdown.

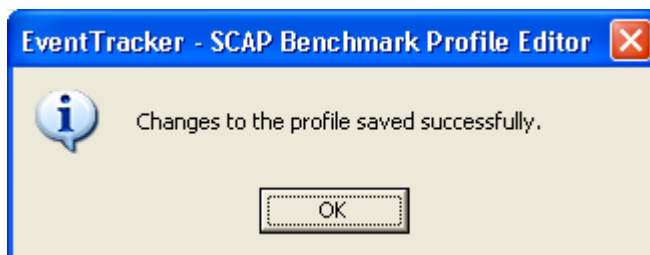
Table 131

Profile element type	Used to
	Select/unselect a rule from a profile. To edit the elements in Idref column, double click on element or

Select	<p>right click on element, and then select Edit.</p> <p>EventTracker displays a message.</p> 
Set-value	<p>Override the default value for a rule in the profile, without changing any of its other properties.</p>
Refine value	<p>Select from a list of value, value for a rule in the profile. To edit the refine value:</p> <p>Double click on element in Idref column or right click on element, and then select Edit.</p> <p>EventTracker displays 'Refine value element properties' pop up.</p>  <p>Select the appropriate option in Selector dropdown.</p>
Refine rule	<p>Override the default properties (severity, weight, role etc) of a rule in the profile. This profile element</p>

- 4 Select or clear the appropriate element checkbox, and then click **Save** to save the changes in existing benchmark list.
- EventTracker displays the confirmation message.

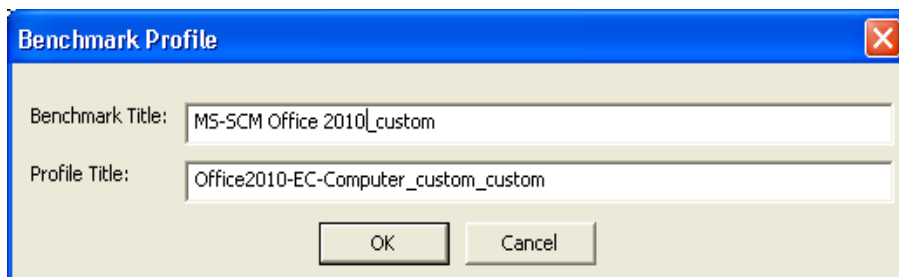
Figure 405



(OR)

Click **Save As**, and you can create a custom benchmark, which will be saved as XML file.

Figure 406
Benchmark Profile



Click **Ok**.

EventTracker displays the confirmation message.

Figure 407



Click **Ok**.

The newly created benchmark can be seen in the **Select benchmark** dropdown.

Figure 408

**Note**

For more information on SCAP, click [here](#).

EventTracker Event Correlator

What is Event Correlation

Event Correlation is the process of analyzing events to identify patterns. This helps pinpoint problems such as abuse, intrusion, attacks, or failure. The real time event correlation simplifies complex events and alerts the enterprise threats.

Event Correlation Engine

Event Correlator module is a part of EventTracker™ product of System-Intelligence suite. Event Correlation Engine (ECE) can be installed on the same system where the EventTracker™ manager is installed or on a different system.

All events from different systems are received by ECE through EventTracker™ Manager. ECE will apply the predefined correlation conditions. Each correlation condition defines a pattern or sequence of events to be checked within a preset time interval, defines rules to be applied and what action needs to be taken.

How Event Correlator works

ECE analyzes the events received from EventTracker based on the rule configurations.

Correlation has the following phases to achieve the Flex Report expected by the user,

- 1 Determining the pattern
 - a. Which Events have to be monitored, how they look like?
 - b. How often do they occur?
 - c. What are the sources of the Events?
- 2 Define the action
 - a. What should be performed as the result of Flex Report for a particular event set?
 - b. Where the result should effect?
- 3 Simulate the conditions

ECE module comes with a large number of default correlation conditions, so your organization can detect most critical conditions right away.

Configuration User Interface

Configuration user interface helps you configure the following attributes for each rule set.

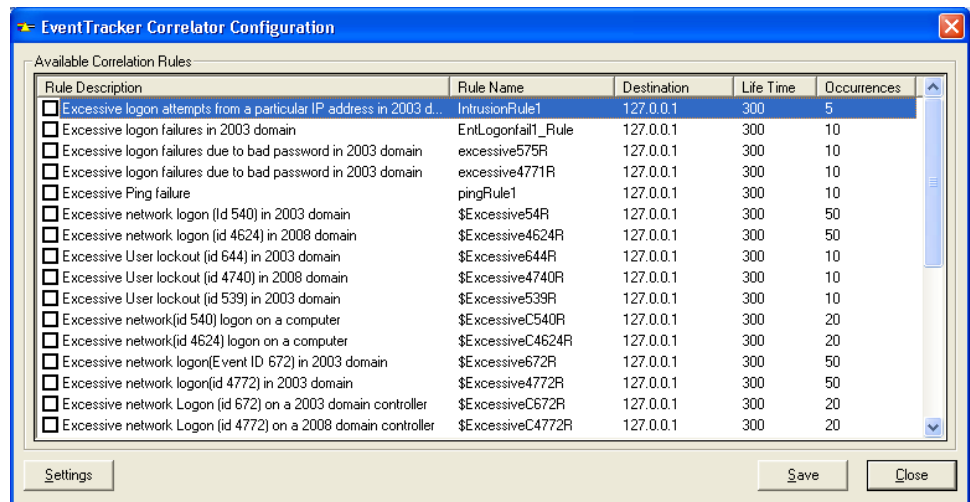
Destination: IP address or name of the system, which receives the resultant events from Event Correlator. This should be a system which is having the EventTracker Manager (receiver) installed.

Life Time: Time (seconds) to check the event's expiry. If the event does not occur within the specified lifetime, it won't be considered for action.

Occurrences: Number of occurrences (count) of the event to monitor. The action will be fired up only when the specified number of events occurred.

- 1 Double-click **Event Correlator** on the EventTracker Control Panel.
EventTracker displays the Correlator Configuration window.

Figure 409
Correlator
Configuration



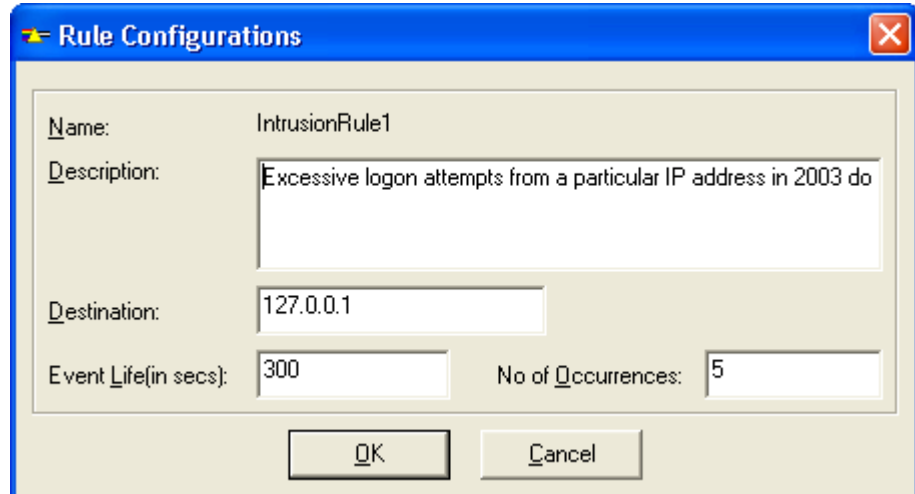
2 Double-click a rule.

(OR)

Select a rule and then click **Settings**.

EventTracker displays the Rule Configurations window.

Figure 410
Rule Configurations



3 Type appropriately in the relevant fields and then click **OK**.

4 Click **Save** on the Correlator Configuration window.

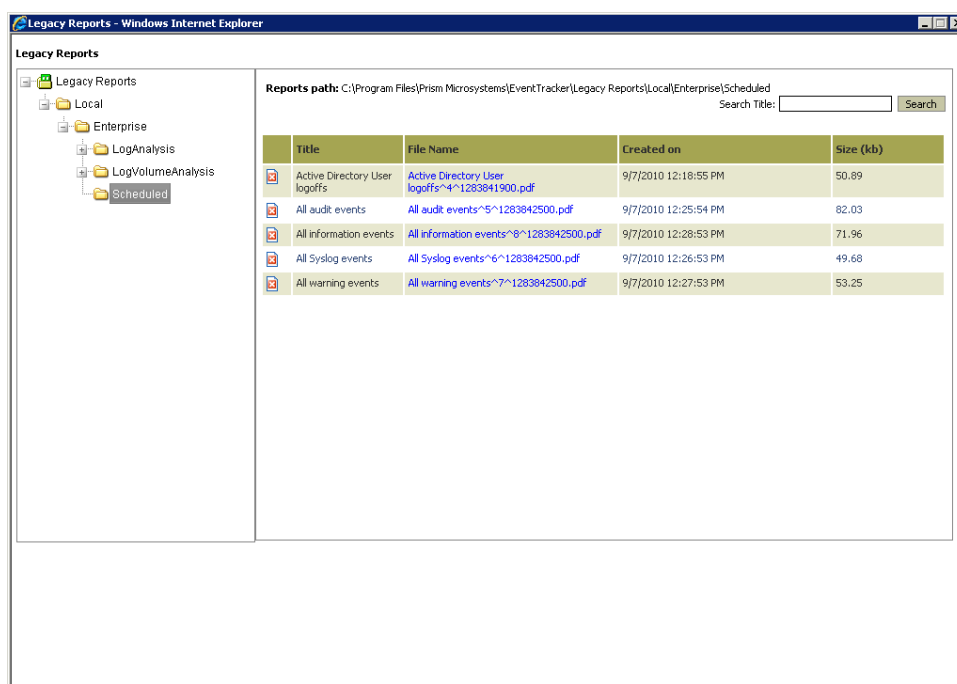
Viewing Published Legacy Reports

This option helps to view Published legacy reports. This feature is available for User who wish to upgrade from version v6.4 to v7.3.

To view published legacy reports

- 1 Click **Tools** at the upper-right corner, and then click **Legacy Reports**.
EventTracker displays the Legacy Reports page.
- 2 Expand the Legacy Reports tree and click an appropriate node.
EventTracker displays the associated reports in the right pane.

Figure 411
Legacy Reports



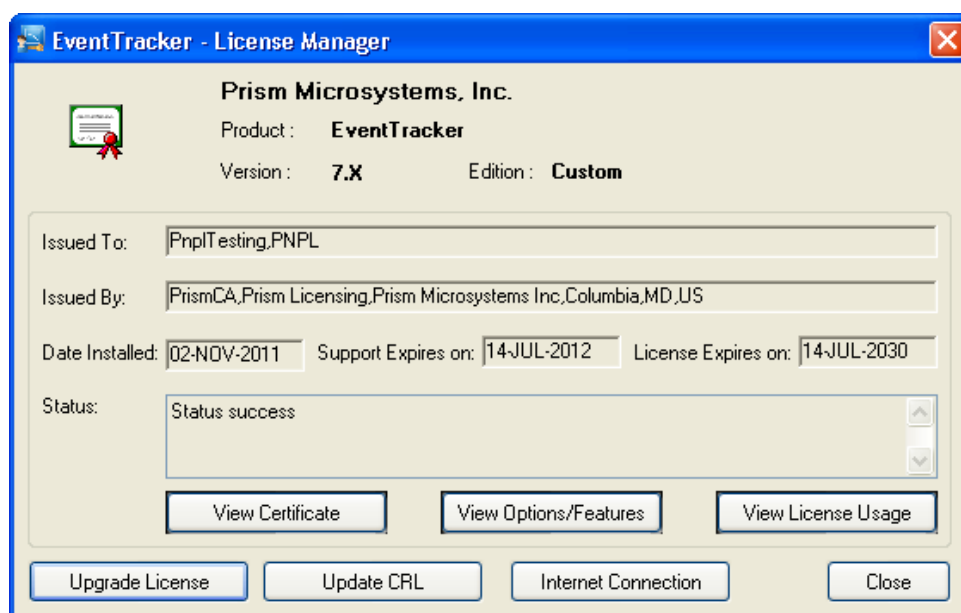
- 3 Click the name of the file in the **File Name** column to view reports.

License Manager

This option helps to upgrade license, view license usage, and update Certificate Revocation List (CRL).

- 1 Double-click **License Manager** on the EventTracker Control Panel

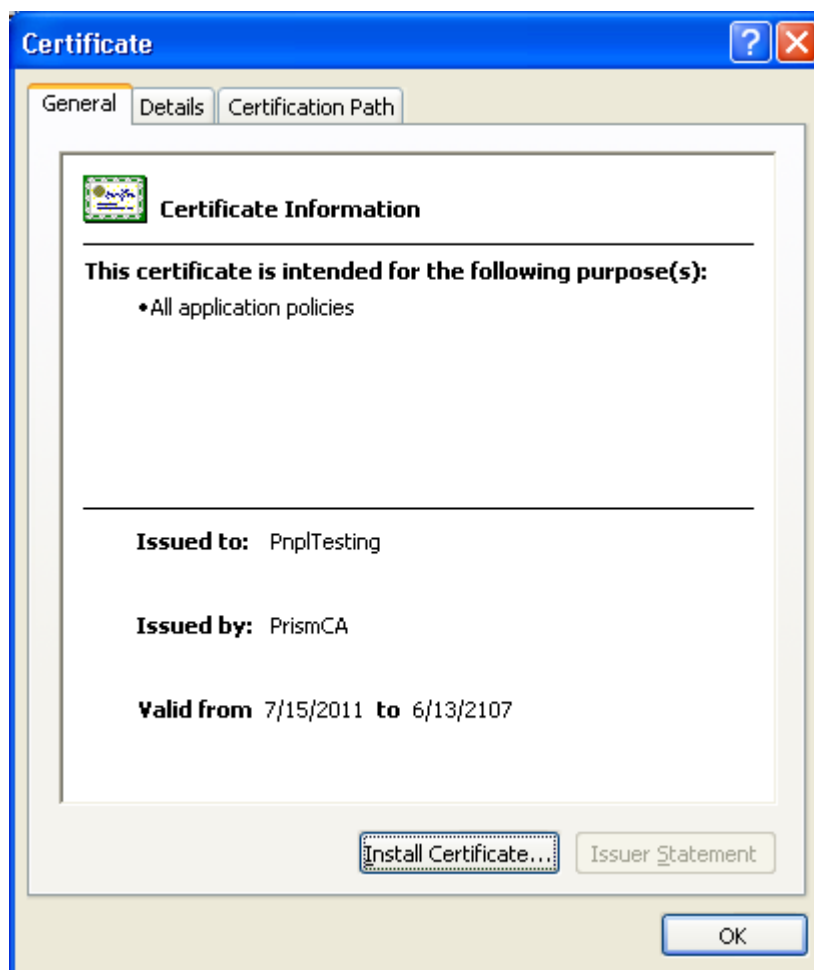
Figure 412
License Manager



- 2 Click **View Certificate**.

EventTracker displays the Windows Certificate Viewer.

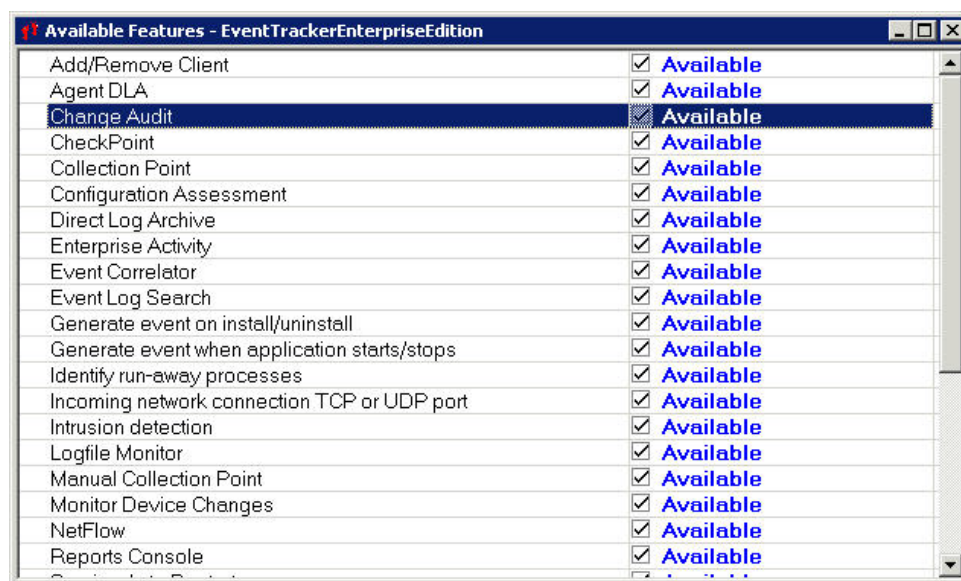
Figure 413
Windows Certificate
Viewer



Click **Install Certificate** button to import certificate to a certificate store.
A certificate store is the system area where the certificates are kept.

- 3 Click **View Options/Features** on the License Manager window.

Figure 414
Available Features



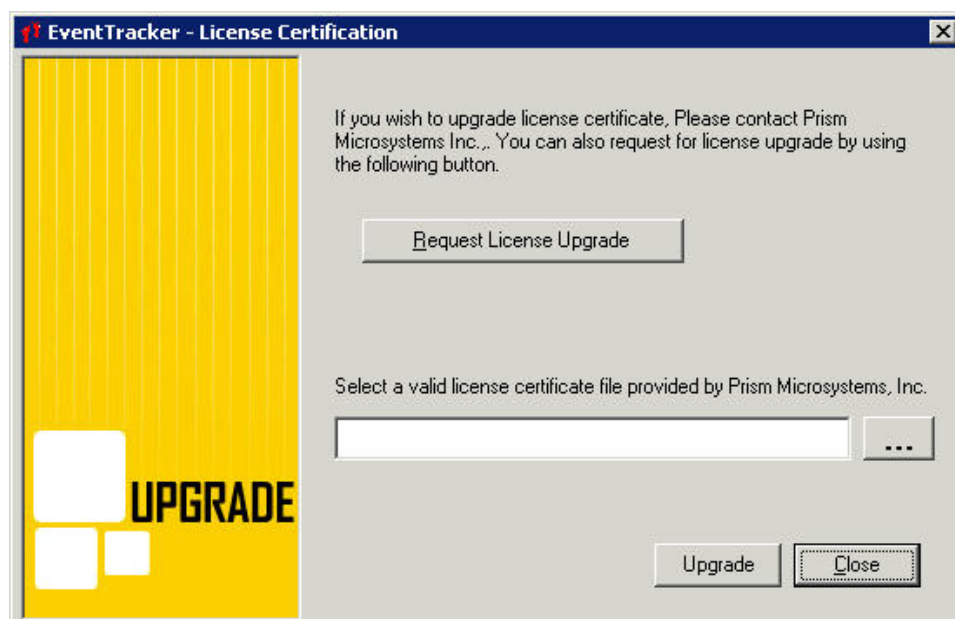
4 Click **View License Usage**.

Figure 415
License Usage

[illegible]

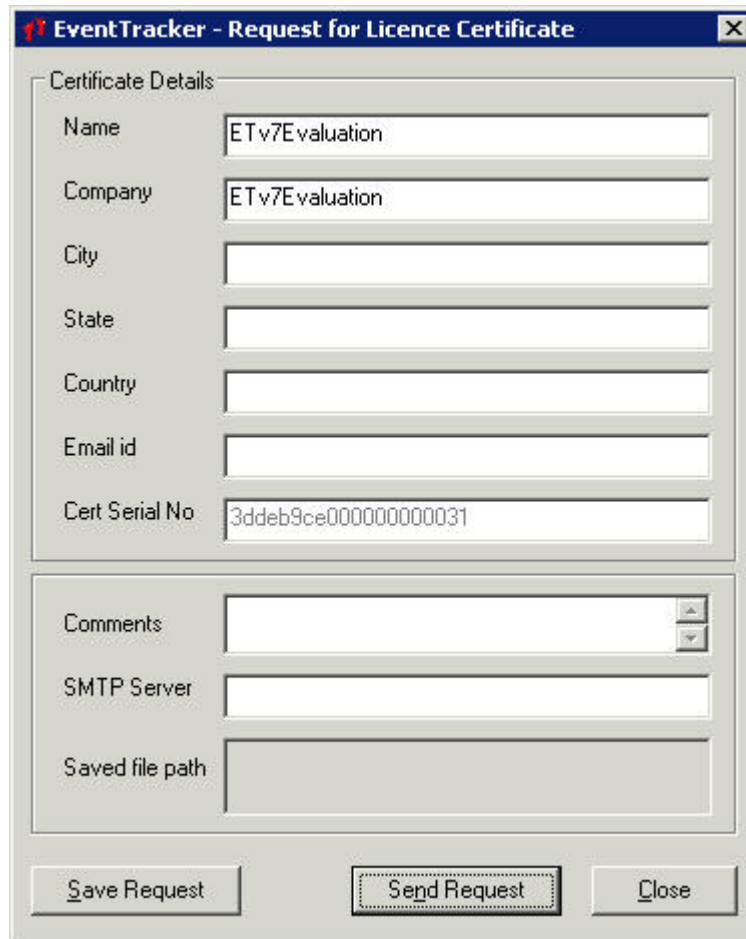
5 Click **Upgrade License**.

Figure 416
License Certification



- 6 Click **Request License Upgrade** to request a new license to upgrade.

Figure 417
Request for License
Certificate



The dialog box is titled "EventTracker - Request for Licence Certificate". It contains two main sections: "Certificate Details" and a section for additional information. The "Certificate Details" section includes fields for Name, Company, City, State, Country, Email id, and Cert Serial No. The "Additional Information" section includes fields for Comments, SMTP Server, and Saved file path. At the bottom, there are three buttons: "Save Request", "Send Request", and "Close".

Certificate Details	
Name	ETv7Evaluation
Company	ETv7Evaluation
City	
State	
Country	
Email id	
Cert Serial No	3ddeb9ce000000000031

Comments	
SMTP Server	
Saved file path	

Buttons: **Save Request** **Send Request** **Close**

- 7 Fill-in appropriately in the relevant fields.
- 8 Click **Save Request** to save the request in Notepad and send it later.
- 9 Click **Send Request** to send E-mail.

(OR)

If you already have a license to upgrade, click the browse button.

EventTracker displays the Open dialog box.

Go to appropriate folder and select the certificate file.

Click **Open**.

Click **Upgrade**.

- 10 Click **Update CRL** on the License Manager window.

A Certificate Revocation List (CRL) is a list of certificate serial numbers which have been revoked, are no longer valid, and should not be relied upon.

A CRL, like a certificate, also has a validity date span. The date span ensures that the CRL is not used after a certain time, but also allows the application checking the CRL to cache the CRL so that it doesn't have to keep downloading it over and over again.

While installing EventTracker, CRL (PrismCA.crl) is downloaded to the default install path typically ...\\Program Files\\Prism Microsystems

EventTracker displays the Open dialog box.

- 11 Select the CRL file and then click **Open**.
-

EventVault Explorer

Existing Report/Log Search architecture goes through the typical CAB file processing for generating report or finding out specific data based on the given criteria. In real time environments (on heavy load scenarios, unknown conditions and multiple searches) this process takes lot of time and does not solve the immediate queries. Easy way to process quickly is to have the archived events in a cache, so that redundant processing of CAB files is eliminated.

Based on the given criteria EventVault generates search result from cache and saves the search results as **Search history** for future reference.

Run ad-hoc reports and save the data in a database. You can further drill-down the cached data by,

- Specifying Location, words, exact word/phrase or range of Event Id, in **Advance search**
- Selecting existing **Category**
- Constructing your own **SQL Query**

User can also configure EventVault Explorer to use remote Sqlserver database. The reason is, SQL Server Express Edition has maximum database size limitation of 4 GB. Hence, to overcome this limitation an option is provided to use Remote Sqlserver, which can be Sqlserver Enterprise Full Edition. Unlike SQL Server Express edition, Sqlserver enterprise edition does not have any size limitation.

Performing search in EventVault Explorer

This option helps you to search CAB files.

Search CAB files, through 'New Search' tab

- 1 Click **Tools** at the upper-right corner and then click **EventVault Explorer**.
EventTracker displays the EventVault Explorer.
- 2 In Duration tab, select the **Interval**.

Figure 418
EventVault Explorer
- Duration

EventVault Explorer Configuration

Search history New search

Duration Systems Refine/Filter

Interval

☒ Select interval: Last 1 Day

☐ Select date range:

From : 9/16/2012 03 : 22 : 18 : PM

[mm/dd/yyyy] [hh:mm:ss]

To : 9/17/2012 03 : 22 : 19 : PM

☐ Limit to time range

Description:

Search Close

3 In Systems tab, select the system(s) / system group(s)/ Sites.

EventVault Explorer Configuration

Search history New search

Duration Systems Refine/Filter

☐ Groups ☒ Systems ☐ All Systems

Search System(s): tip

☒ Default ☐ TOONS

☒ Realtime ☐ File Transfer View all systems

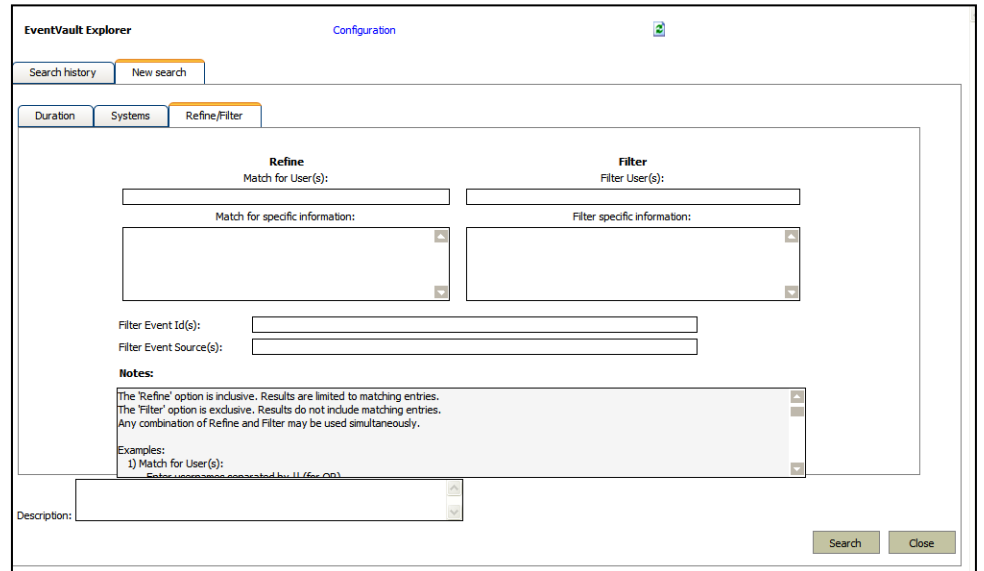
Description:

Search Close

Figure 419
EventVault Explorer
- System

4 Set the **Refine / Filter** criteria.

Figure 420
EventVault Explorer
– Refine/Filter



EventVault Explorer Configuration

Search history | New search

Duration | Systems | **Refine/Filter**

Refine
Match for User(s):
Match for specific information:
Filter Event Id(s):
Filter Event Source(s):

Filter
Filter User(s):
Filter specific information:

Notes:
The 'Refine' option is inclusive. Results are limited to matching entries.
The 'Filter' option is exclusive. Results do not include matching entries.
Any combination of Refine and Filter may be used simultaneously.

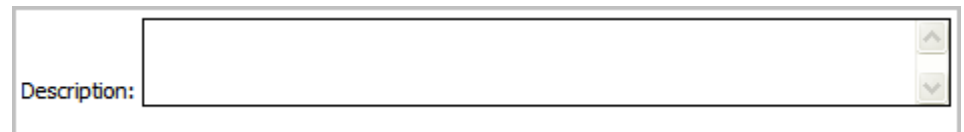
Examples:
1) Match for User(s):
Enter username associated with IT (few Q&A)

Description:

Search Close

- 5 Type an appropriate **Description**.

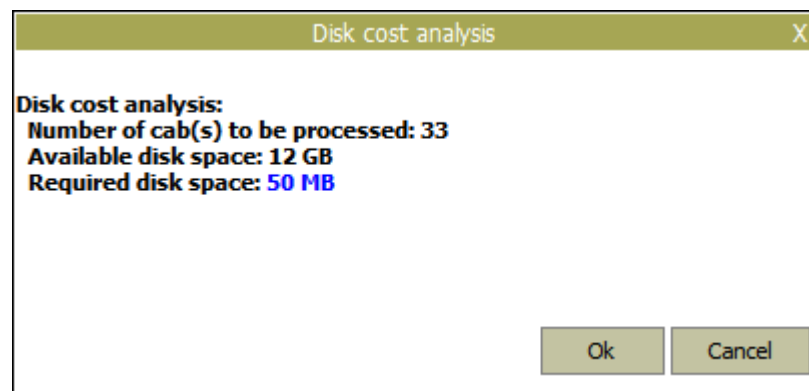
Figure 421
EventVault Explorer
– Description



Description:

- 6 Click **Search**.
EventTracker displays the Disk cost analysis pop-up window.

Figure 422
Disk Cost Analysis



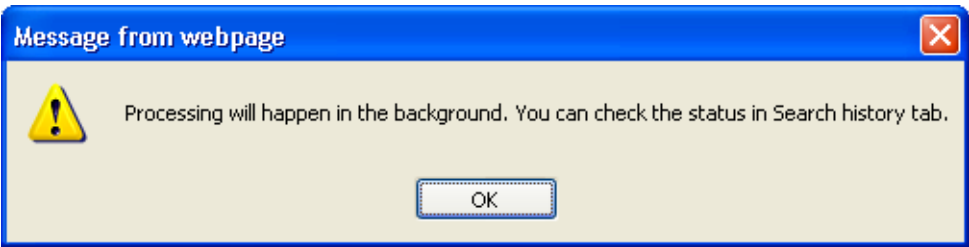
Disk cost analysis X

Disk cost analysis:
Number of cab(s) to be processed: 33
Available disk space: 12 GB
Required disk space: 50 MB

Ok Cancel

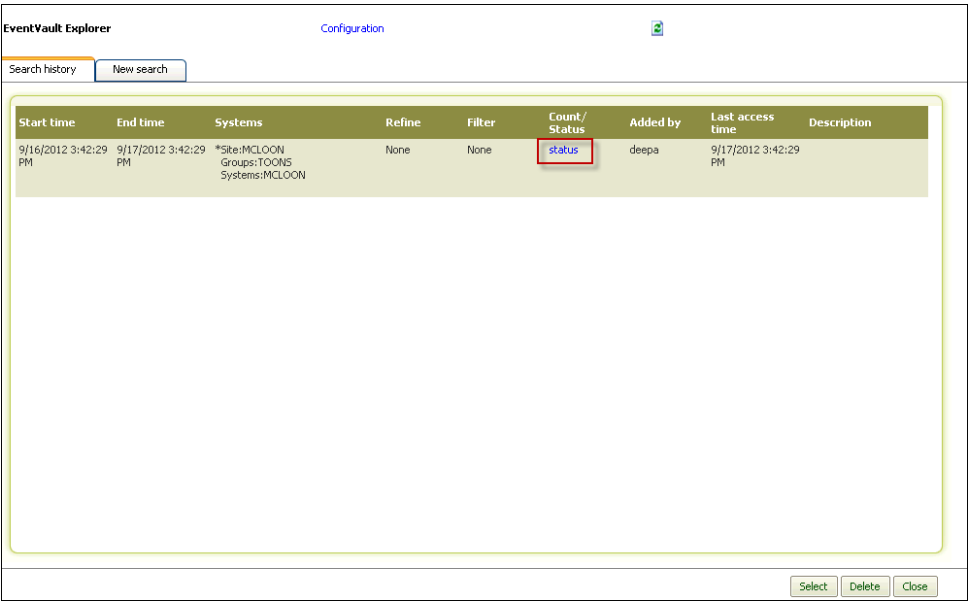
- 7 Click **OK**.
EventTracker displays information message box.

Figure 423



- 8 Click **OK**.
- EventTracker displays **Search History** tab with the result set.

Figure 424
EventVault Explorer-
Search History tab



- 9 Click the **Status** hyperlink.
- EventTracker displays EventVault Explorer processing status window.

Figure 425
EventVault Explorer
processing status
window

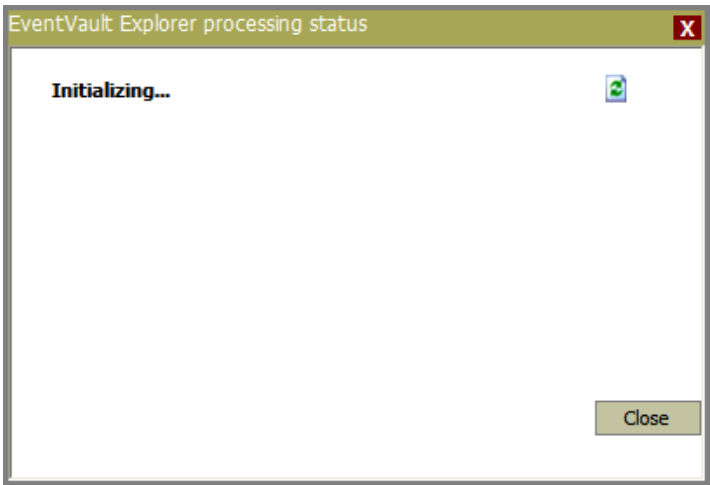


Table 132

Status	For
Initializing	New request
Processing	Cab Extraction
Exception Occurred	Failed
Status of unpacking Archives	All the archives have been processed (unpacked) successfully.

Search CAB files, through ‘Search History’ tab

As said earlier, EventTracker saves all your queries and the result set in the data cache. You can reuse the data to further refine the search.

- 1 Open **EventVault Explorer**.
- 2 Click the **Search History** tab, if not selected.

EventTracker displays Search History tab with all search queries framed earlier.

Figure 426
Search history tab

EventVault Explorer - Windows Internet Explorer

EventVault Explorer Configuration

Search history New search

Start time	End time	Systems	Refine	Filter	Count/Status	Added by	Last access time	Description
9/3/2011 12:29:00 PM	9/5/2011 12:29:00 PM	*Site:SAFARI Groups:Default Systems:ESXWIN2K3VM6, SAFARI	None	None	status	Sonal	9/5/2011 12:30:42 PM	
9/3/2011 12:28:27 PM	9/5/2011 12:28:27 PM	*Site:SAFARI Groups:TOONS Systems:DEXTER, SAFARI	None	None	15,040	Sonal	9/5/2011 12:31:06 PM	
8/22/2011 12:28:02 PM	9/5/2011 12:28:02 PM	*Site:SAFARI Groups:Default Systems:DEXTER, ESXWIN2K3VM6, SAFARI	None	None	65,787	Sonal	9/5/2011 12:42:06 PM	

Select Delete Close

- 3 Select a query and then click **Select**.
EventTracker displays the **Refine Criteria** pop-up window with log count.

Figure 427
Refine Criteria
Window

Refine Criteria - Windows Internet Explorer

EventVault Explorer

Metadata Advanced Search Category SQL Query

Total log count: 15,040

Log type (Tag)

- ☐ Application (4,945)
- ☐ Application (9,890)
- ☐ Security (2,561)
- ☐ Security (5,122)
- ☐ System (14)

Event type (Tag)

- ☐ Audit Failure (100)
- ☐ Audit Failure (50)
- ☐ Audit Success (2,511)
- ☐ Audit Success (5,022)
- ☐ Error (43)

Category (Tag)

- ☐ 0 (9,770)
- ☐ 3 (16)
- ☐ 6 (16)
- ☐ 7 (20)
- ☐ 4 (12)

Event id (Tag)

- ☐ 3 (2)
- ☐ 8 (16)
- ☐ 16 (2)
- ☐ 20 (2)
- ☐ 100 (2)

Event source (Tag)

- ☐ crypt32 (16)
- ☐ crypt32 (16)
- ☐ EventTracker (9,874)
- ☐ EventTracker (9,874)
- ☐ HTTP (2)

Domain (Tag)

- ☐ N/A (62)
- ☐ N/A (62)
- ☐ NT AUTHORITY (14,352)
- ☐ NT AUTHORITY (14,352)
- ☐ SAFARI (10)

System (Tag)

- ☐ DEXTER (9,146)
- ☐ DEXTER (9,146)
- ☐ SAFARI (5,894)
- ☐ SAFARI (5,894)

User (Tag)

- ☐ ASPNET (10)
- ☐ ASPNET (10)
- ☐ HARISH (214)
- ☐ HARISH (214)
- ☐ LOCAL SERVICE (12)

From: 9/3/2011 12:28:27 PM To: 9/5/2011 12:28:27 PM

Search New search Close

Search criteria

Time range	Systems	Refine	Filter	Description
Start time: 9/3/2011 12:28:27 PM End time: 9/5/2011 12:28:27 PM	*Site:SAFARI Groups:TOONS Systems:DEXTER, SAFARI	Refine user: None Refine info:	Filter user: None Filter info: None	

Table 133

Field	Description
Metadata	Metadata displays event properties and its count in the search result. You can further narrow down the search criteria by selecting specific event properties.
Advanced Search	Refer Advanced Search section in the Log Search user guide .
Category	Select a Category or Categories to search associated events.
SQL Query	Select this option to frame your own query. Available fields in the logs selected are displayed to aid you in framing queries. Follow the examples to avoid errors and make sensible yet powerful queries.

- 4 Click the **New Search** button to go the **New Search** tab in EventVault Explorer.

OR

Click **Search** to see the search result based on the given search criteria.

EventTracker displays the result set.

Note



EventTracker saves the searches in the database.

Configuring EventVault Explorer to use remote Sqlserver

Before you begin, read the below points carefully.

Note



- MS Sqlserver Enterprise 2005 or 2008 are supported.
- For best performance the instance of Sqlserver Enterprise should be dedicated for this usage.
- The Sqlserver instance should be accessible from the EventTracker server, preferably via fully qualified domain name (FQDN).
- Windows authentication is used for connecting to the Sqlserver.

For successful configuration, follow the steps given below:

In Sqlserver system,

- Grant user (User used for EventTracker configuration) Sysadmin access on remote Sqlserver.
- Create folder on remote Sqlserver system to store EventVault Explorer database file and give user (User used for EventTracker configuration) full access on folder created on remote system.

In EventTracker server

Click the **'Tools'** dropdown on the control panel and then click on **'EventVault Explorer'**.

The **EventVault Explorer window** will appear on the screen (See Figure 456).

Figure 428
EventVault Explorer
Window

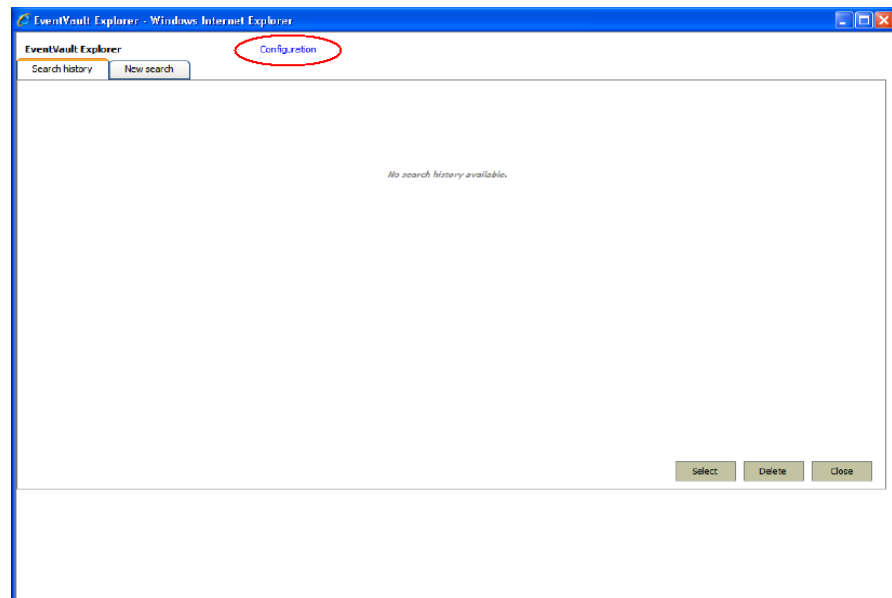


Figure 429
Run Dialog box

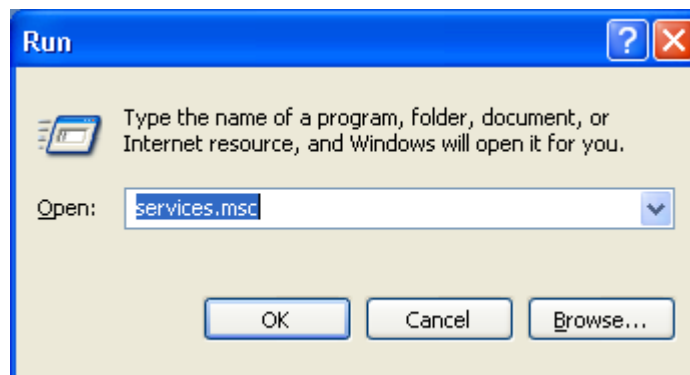


Figure 430
EventVault Explorer
- Configuration Pop
up Window

Click the 'Configuration' hyperlink. (See Figure 456- Marked with red circle)
EventVault Explorer Configuration pop up window appears on the screen.

EventVault Explorer Database Configuration

This feature will unpack log data from the compressed archives to an instance of MS SQL server.
The instance of SQL Express installed on the EventTracker server (used to store configuration), may be used but not recommended.
An instance of SQL Enterprise 2005/8 is preferable.

☒ SQL Server Enterprise

Host server name : SQL server instance name : (blank incase of default instance)

Database path :

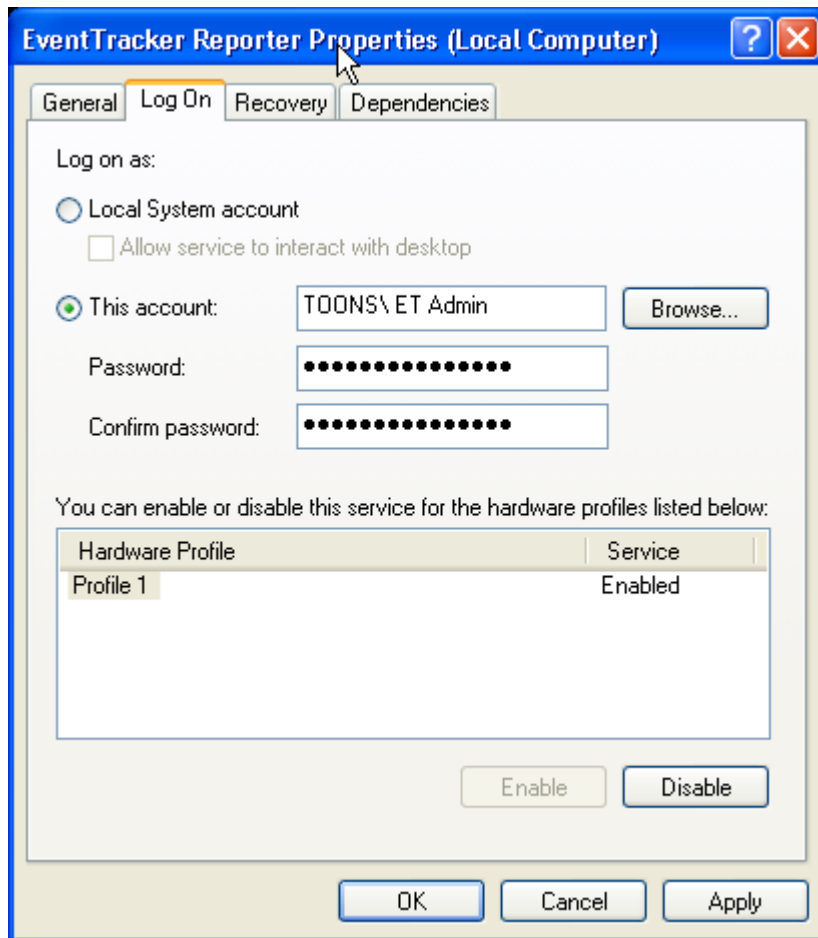
Important :

- 1) MS SQL Server Enterprise 2005 or 2008 are supported.
For best performance the instance of SQL Server Enterprise should be dedicated for this usage.
- 2) The SQL server instance should be accessible from the EventTracker server, preferably via FQDN.
- 3) Database path on the SQL Server instance should be provided. Example: D:\EventVaultDB.
Shared path is not supported.
- 4) Windows authentication is used for connecting to the SQL Server.
The account "TOONS\ET Admin" should be granted admin privileges on the SQL Server and full permissions on the database path folder.
- 5) The "EventTrackerReporter" service should be running with "TOONS\SONAL" account.

Max history count :

Select 'EventTracker reporter' from Services window.

Figure 432
EventTracker
Reporter Properties
window



Click the **'Apply'** button, and then click the **'OK'** button.

Note



For more details, refer [EventVault Explorer – Introduction and Usage document](#).

Chapter 21

Managing Users

In this chapter, you will learn how to:

- [Elevate a normal user as an EventTracker Administrator](#)

EventTracker Roles, Permissions & Privileges

Roles

Role can be defined in terms of the authorization and obligation policies for a particular job function, which specify what actions the user is permitted or is obliged to do.

Fine-grained role based security model secures the content of the application and the enterprise network at large.

Privileges

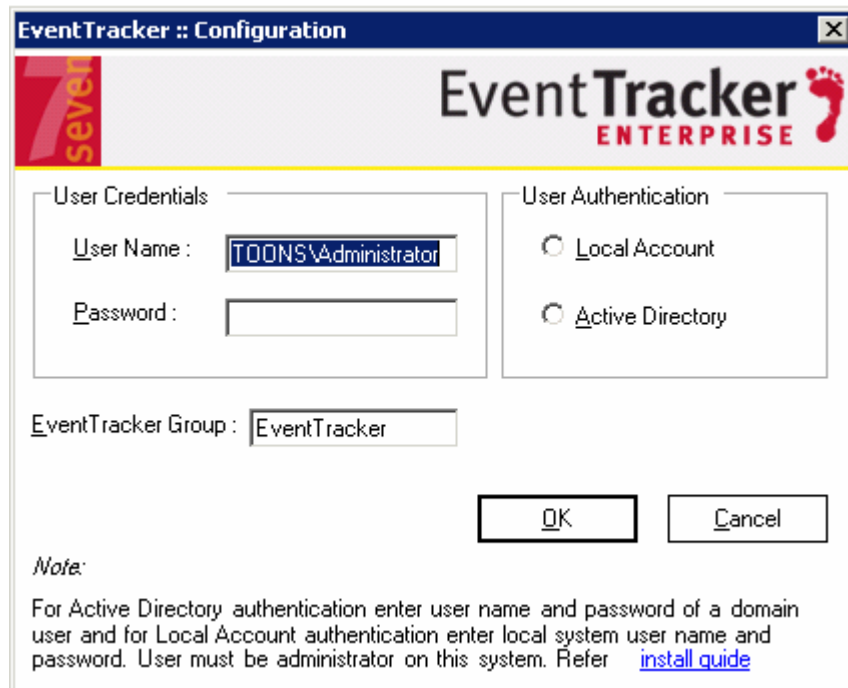
Privileges are the rights granted to roles to access EventTracker modules.

Permissions

Permissions are the rights granted to users to access computer groups.

While installing, EventTracker prompts you to enter name of the EventTracker Group, valid User Credentials, and select User Authentication type.

Figure 433
EventTracker
Configuration



The image shows the 'EventTracker :: Configuration' dialog box. It has a title bar with the text 'EventTracker :: Configuration' and a close button. The dialog is divided into two main sections: 'User Credentials' and 'User Authentication'. In the 'User Credentials' section, there are two text boxes: 'User Name' containing 'TOONS\Administrator' and 'Password' which is empty. In the 'User Authentication' section, there are two radio buttons: 'Local Account' (selected) and 'Active Directory'. Below these sections is a text box for 'EventTracker Group' containing 'EventTracker'. At the bottom right are 'OK' and 'Cancel' buttons. At the bottom left, there is a 'Note:' section with text explaining the requirements for Active Directory and Local Account authentication, and a link to the 'install guide'.

EventTracker :: Configuration

User Credentials

User Name : TOONS\Administrator

Password :

User Authentication

☒ Local Account

☐ Active Directory

EventTracker Group : EventTracker

OK Cancel

Note:

For Active Directory authentication enter user name and password of a domain user and for Local Account authentication enter local system user name and password. User must be administrator on this system. Refer [install guide](#)

Note



Whenever you change the EventTracker logon password, please update the same in **EventTracker Configuration**. You can find EventTracker configuration in Start > Programs > Prism Microsystems > EventTracker > EventTracker Configuration

By default, this user is assigned administrator role. You cannot view / modify privileges and permissions of administrators.

An administrator can:

- 1 Access all modules and system groups
- 2 Promote a non-admin user as an administrator
- 3 Demote an administrator
- 4 Grant / revoke permissions and privileges to non-admin users

A non-Admin user

- 1 Cannot access the EventTracker Web Control Panel
- 2 is restricted to the permissions and privileges granted

Even if the user is a member of EventTracker User Group, EventTracker denies access if the user is not explicitly granted permissions and privileges.

Figure 434
No Permissions and
Privileges

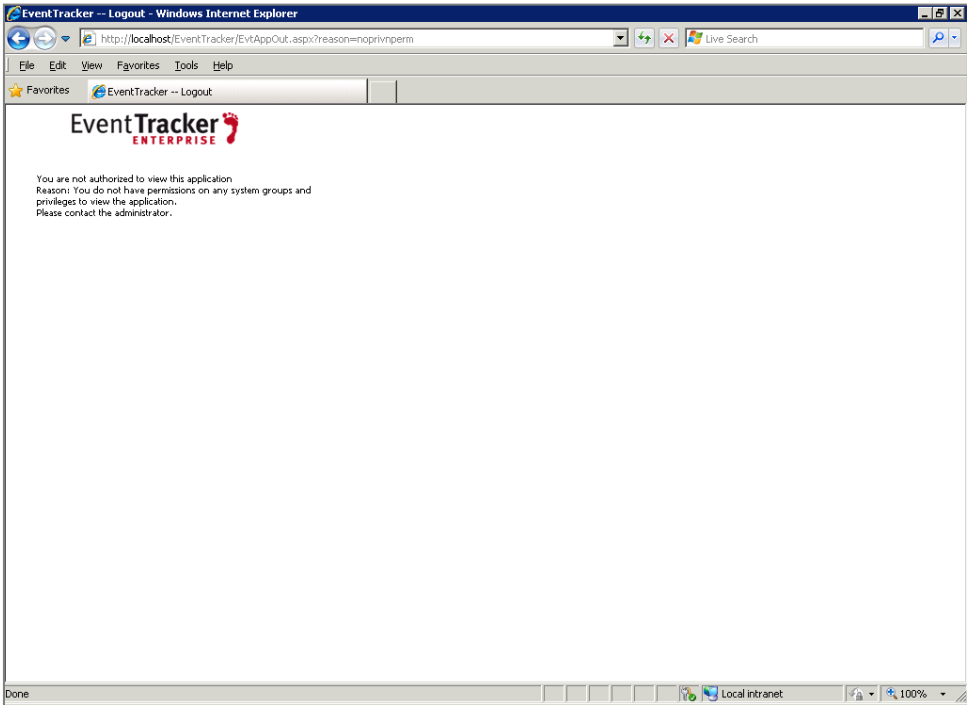


Figure 435
No Privileges

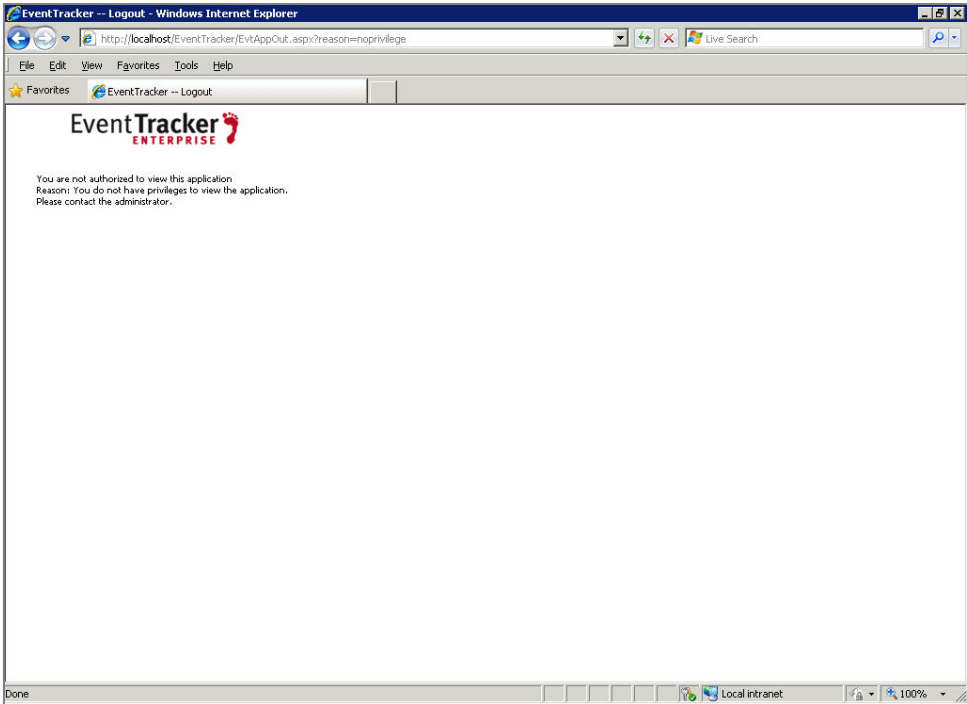
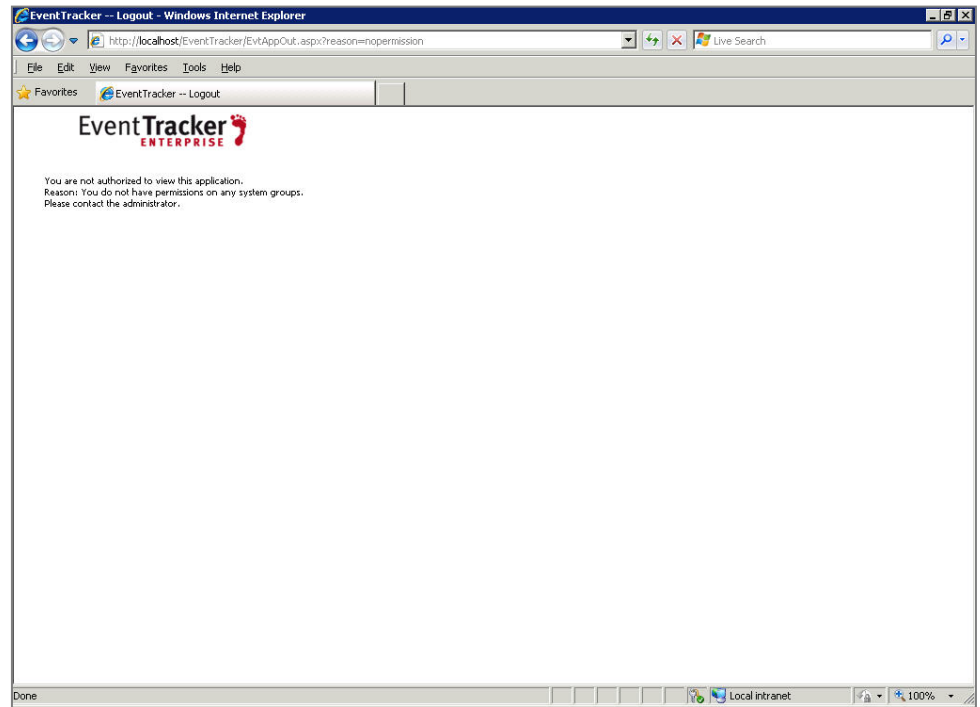


Figure 436
No Permissions



Promoting a Non-Admin User as an Administrator

This option helps to promote a non-admin user as an administrator.

To promote a non-admin user

- 1 Log on to EventTracker Enterprise.
- 2 Click **Admin** dropdown, and then click **Users**.
EventTracker displays the User Management page.

Figure 437
User Management

PRISM

Microsystems

Welcome Deepa Kirana

News

Admin

Tools

Help

Incidents

Status

Behavior

Dashboard

Netflow

Search

Reports

My EventTracker

Change Audit

Config Assessment

User Management

Export

Login Name▲	User Name	Administrator	Interactive User
Administrator	Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Akriti	Akriti Krishna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
akshatha	Akshatha Ananth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
anand	Anand	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ananth	ananth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
bharath	Bharath YR.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Deepa	Deepa Kirana	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
deepak	Deepak Jha	<input type="checkbox"/>	<input checked="" type="checkbox"/>
deepakj1	Deepkj1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
deepakj2	Depakj2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
demouser	Demouser	<input type="checkbox"/>	<input checked="" type="checkbox"/>
elctest1	elctest1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
elctest2	Elctest2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
elctest45	ELC Test45 tyhijnvbghtrcvhndsfvcxa ertyuioilkmnb	<input type="checkbox"/>	<input checked="" type="checkbox"/>
etadmin	ETAdmin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ganesh	S Ganesh	<input type="checkbox"/>	<input checked="" type="checkbox"/>

EventTracker

Microsystems

Server Time: 09/18 02:58:43 PM

Response: 6.968 sec

© Copyright 1999 - 2012 Prism Microsystems, Inc.

If you have license for XmlAPI feature, EventTracker displays an additional column 'Interactive User'. By default, all members of EventTracker Group are interactive users. Interactive users can access the EventTracker application and non-interactive users can access EventTracker API.

Figure 438
User Management

PRISM

Microsystems

Welcome Deepa Kirana

News

Admin

Tools

Help

Incidents

Status

Behavior

Dashboard

Netflow

Search

Reports

My EventTracker

Change Audit

Config Assessment

User Management

Export

Login Name▲	User Name	Administrator	Interactive User
Administrator	Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Akriti	Akriti Krishna	<input type="checkbox"/>	<input checked="" type="checkbox"/>
akshatha	Akshatha Ananth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
anand	Anand	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ananth	ananth	<input type="checkbox"/>	<input checked="" type="checkbox"/>
bharath	Bharath YR.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Deepa	Deepa Kirana	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
deepak	Deepak Jha	<input type="checkbox"/>	<input checked="" type="checkbox"/>
deepakj1	Deepkj1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
deepakj2	Depakj2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
demouser	Demouser	<input type="checkbox"/>	<input checked="" type="checkbox"/>
elctest1	elctest1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
elctest2	Elctest2	<input type="checkbox"/>	<input checked="" type="checkbox"/>
elctest45	ELC Test45 tyhijnvbghtrcvhndsfvcxa ertyuioilkmnb	<input type="checkbox"/>	<input checked="" type="checkbox"/>
etadmin	ETAdmin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ganesh	S Ganesh	<input type="checkbox"/>	<input checked="" type="checkbox"/>

EventTracker

Microsystems

Server Time: 09/18 02:58:43 PM

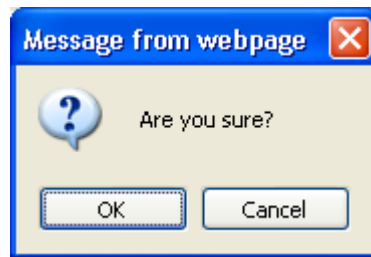
Response: 6.968 secs

© Copyright 1999 - 2012 Prism Microsystems, Inc.

Clear the Interactive User checkbox against the user you wish to make non-interactive.

EventTracker displays the confirmation message box.

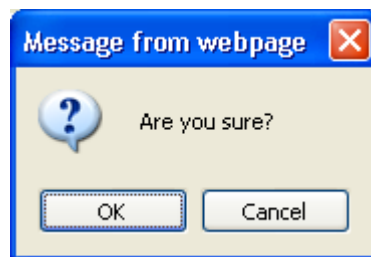
Figure 439
Scenario



- 3 Under **Administrator**, select the checkbox against the user you wish to promote as an administrator.

EventTracker displays the confirmation message box.

Figure 440
Scenario 1



- 4 Click **OK**.

EventTracker elevates the user as an administrator.

Demoting an Administrator

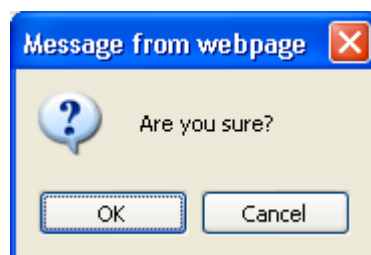
This option helps to demote an administrator.

To demote an administrator

- 1 Clear the checkbox against the admin user that you wish to demote.

EventTracker displays the confirmation message box.

Figure 441



- 2 Click **OK**.

EventTracker demotes the administrator.

Note

When an admin user is demoted, EventTracker revokes privileges on all EventTracker modules and permission on all system groups.

Assigning Permissions to Non-Admin Users

This option helps to assign permissions to non-admin users on enterprise system groups.

To assign permissions

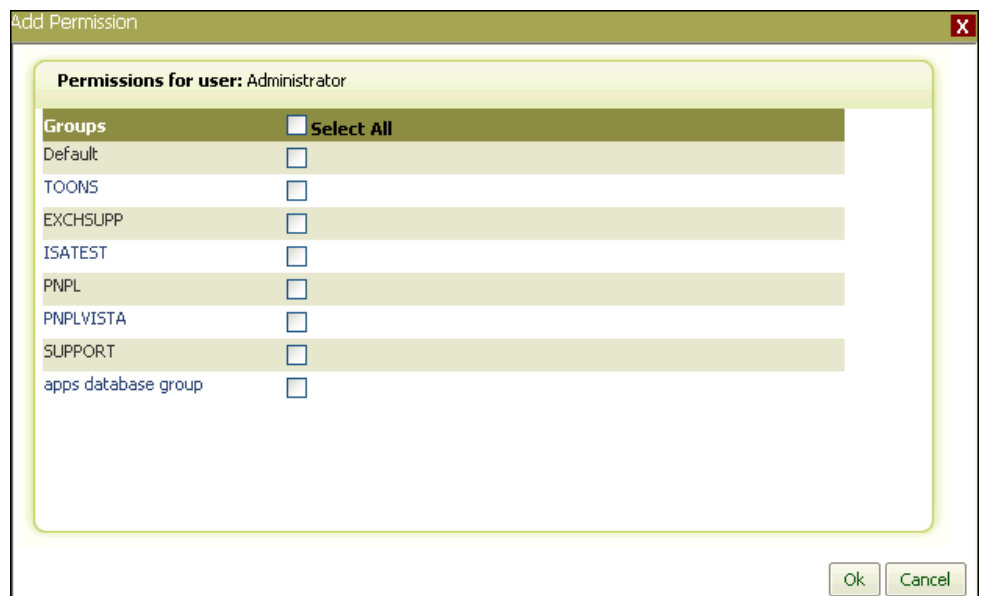
- 1 Move the mouse pointer over the user name that you want to assign permissions.

EventTracker displays the drop-down list.

- 2 Select **Assign Permission** from the drop-down list.

EventTracker displays the Add Permission window.

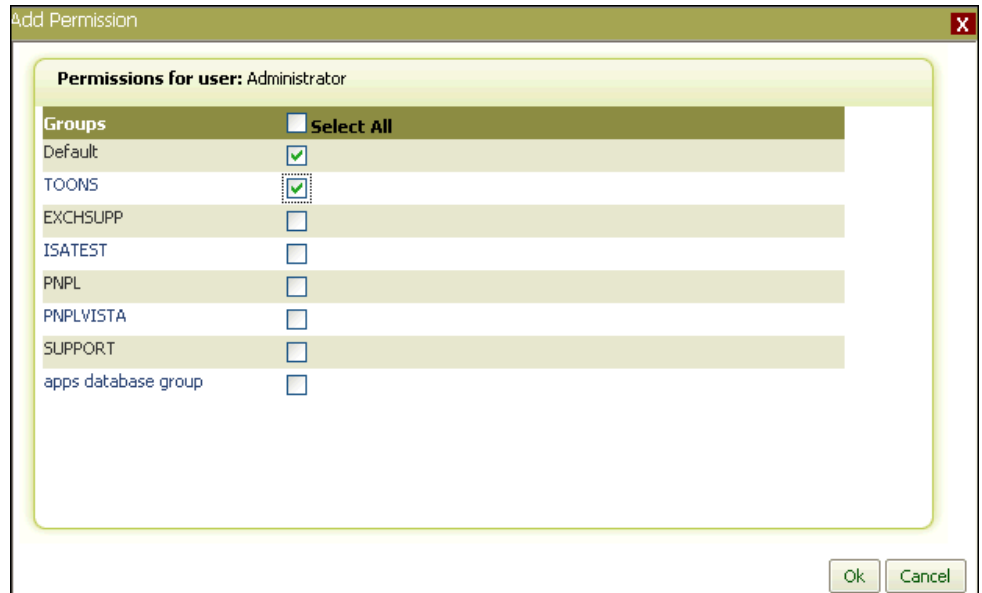
Figure 442
Add Permission



- 3 Select the checkbox against **Select All** to select all system groups.
(OR)

Select the checkbox against the desired system group.

Figure 443
Add Permission



4 Click **OK**.

Viewing Permissions

This option helps to view permissions assigned to non-admin users on enterprise system groups.

To view permissions

- 1 Move the mouse pointer over the user name that you want to assign permissions.
EventTracker displays the drop-down list.
- 2 Select **View Permissions** from the drop-down list.
EventTracker displays the View Permission window.

Assigning Privileges to Non-Admin Users

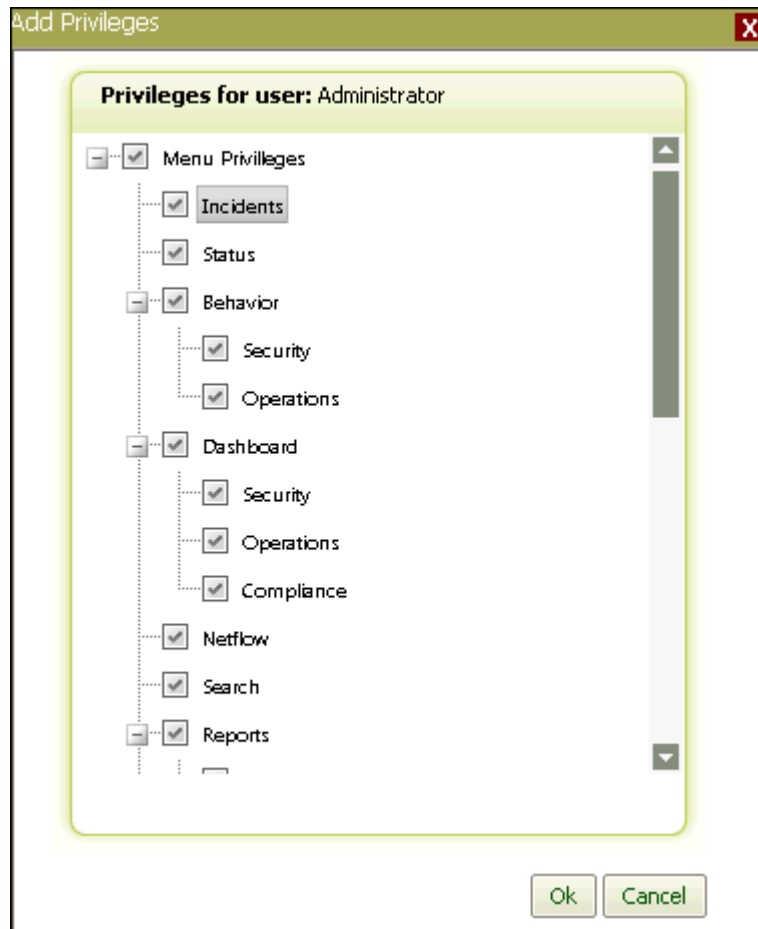
This option helps to assign access privileges to non-admin users on EventTracker modules.

To assign privileges

- 1 Move the mouse pointer over the user name that you want to assign permissions.
EventTracker displays the drop-down list.

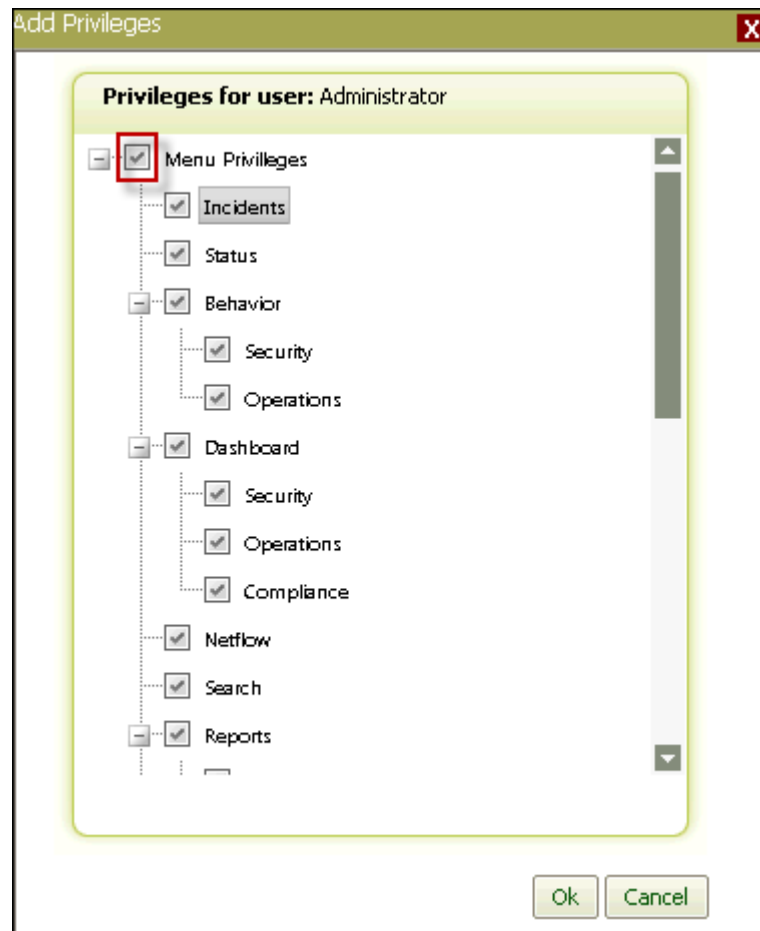
- 2 Select **Assign Privileges** from the drop-down list.
EventTracker displays the Add Privileges window.

Figure 444
Add Privileges



- 3 Click on the check box against the module that you wish to grant access to the user.

Figure 445
Add Privileges



4 Click **OK**.

Viewing Privileges

This option helps to view access privileges assigned to users on EventTracker modules.

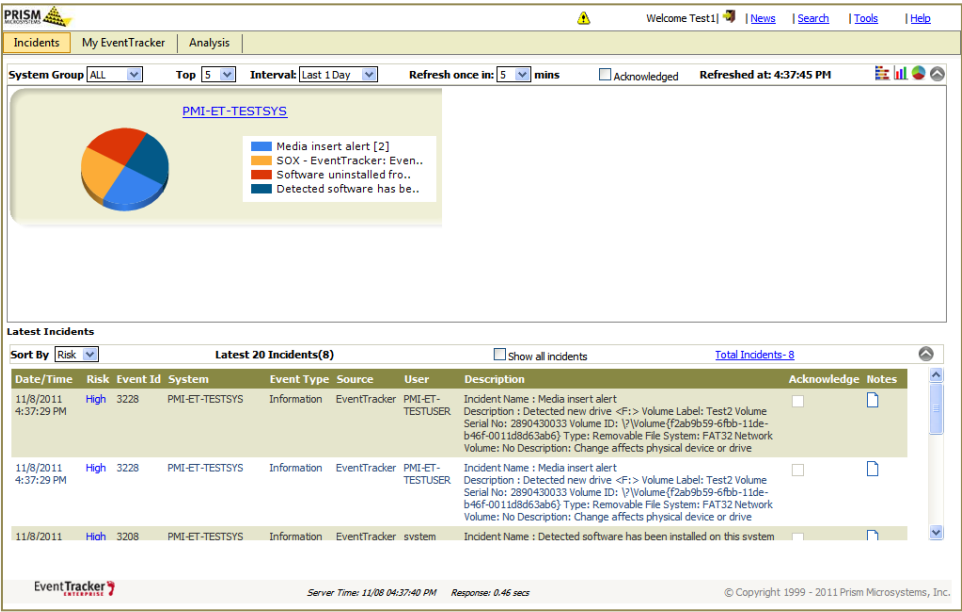
To view privileges

- 1 Move the mouse pointer over the user name that you want to assign permissions.
EventTracker displays the drop-down list.
- 2 Select **View Privileges** from the drop-down list.
EventTracker displays the View Privileges window.

Verification

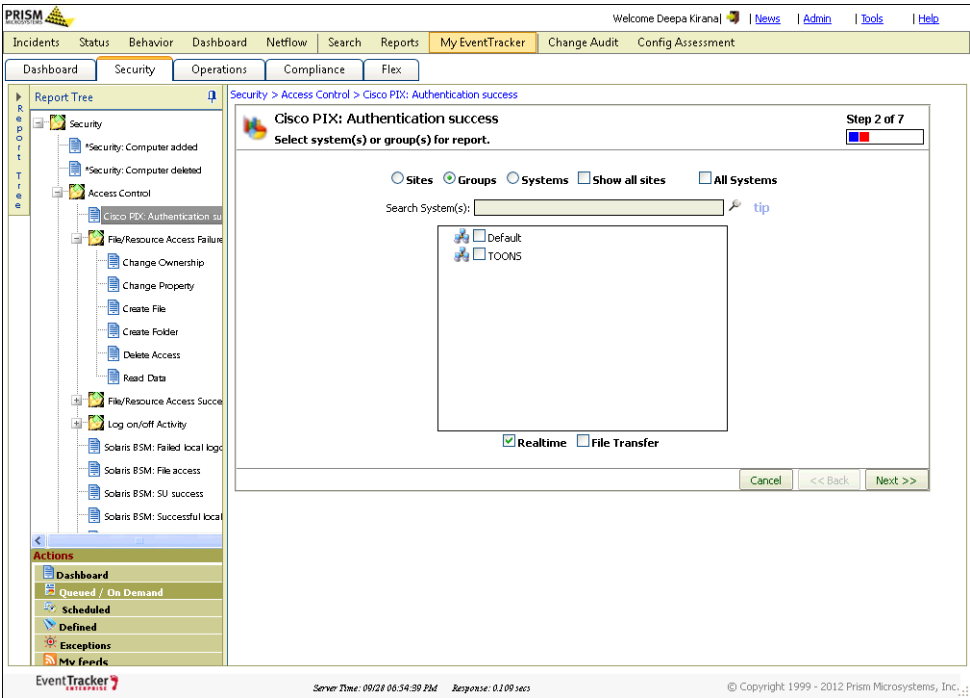
- 1 Log on to EventTracker Enterprise with the user credentials that you have modified. Ex: Administrator.

Figure 446
Home page



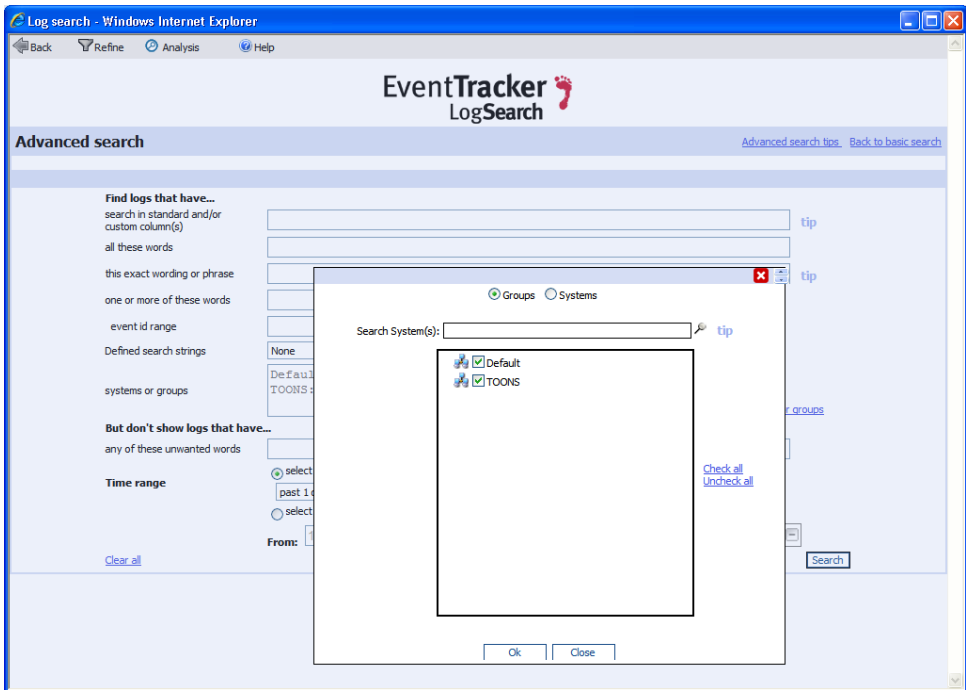
- 2 Configure an On Demand report.

Figure 447
Reports



3 Try Advanced Log Search.

Figure 448
Advanced Log
Search



It is evident from the above figures user is restricted only to the modules and system groups that are allowed to access.

Chapter 22

Collection Point Model

In this chapter, you will learn about:

- [Collection Point model](#)

What is Collection Point model

As the volume of event logs and the complexity of corporate network infrastructure grow day-by-day at an unfathomable rate, mining the esoteric event log data becomes a taxing task for the network administrator. Prism recognized the gravity of the issue and came up with a holistic and single view management model called Collection Point model.

Collection Point model facilitates you to collect cab files from geographically or logically dispersed branch offices and generate consolidated audit reports from a centralized location. Collection Point works on a client-server model, whereby the Collection Points (clients) installed at the branch office locations periodically send the cab files to the Collection Master (server) installed at the corporate headquarters.

Since Collection Point model utilizes TCP as a transport layer, Collection Master (server) acknowledges every packet sent by Collection Points (clients). This assures recovery from data that is damaged, lost, duplicated, or delivered out of order by the Internet communication system. Moreover, the encryption mechanism assures the confidentiality and integrity of data is not compromised while it traverses through the public network. Every Collection Point (client) can be configured to report up to five Collection Masters (servers) simultaneously.

Standard Console

Best suited for (single-level) flat topologies where all monitored nodes report directly to one or more EventTracker Managers.

Collection Master Console

Best suited for hierarchical topologies. Being designated as a Collection Master, receives archives (CAB files) replicated by Collection Points.

Collection Point Console

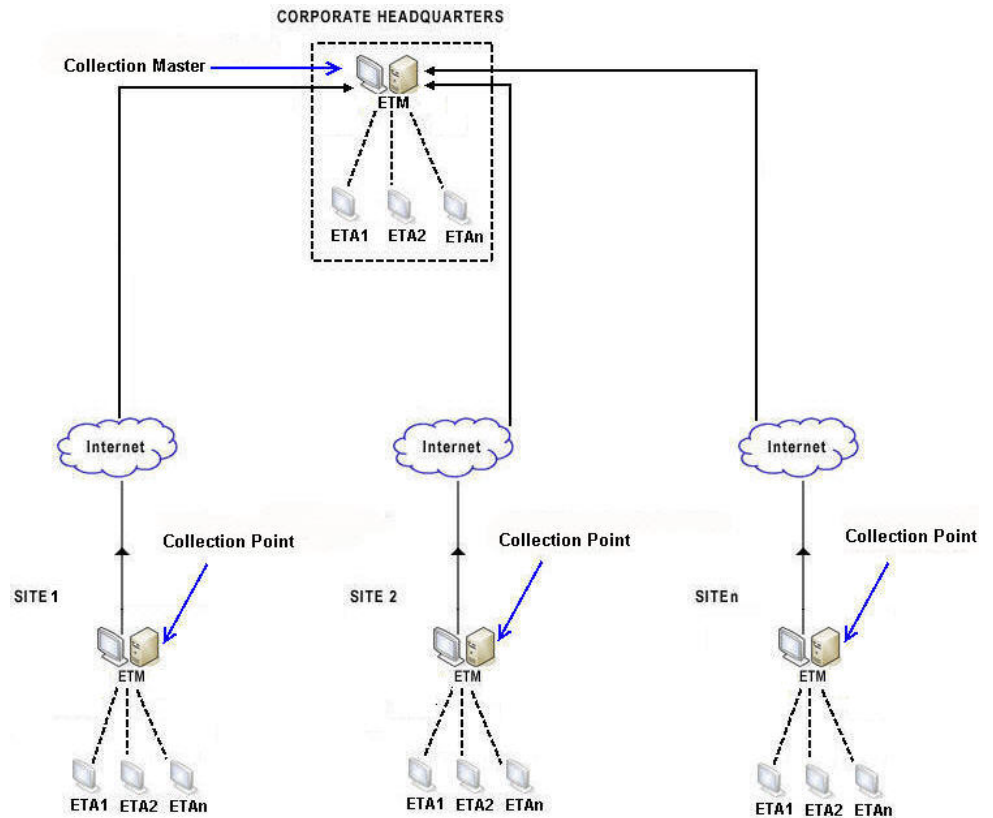
Best suited for hierarchical topologies where all monitored nodes report directly to a local EventTracker Manager, which is designated as a Collection Point, replicates archives (CAB files) to one or more Collection Masters.

Scalability

Collection Point model is best suited for organizations having multiple sites. The sites may geographically spread across the globe or do exist in the same precinct but with a robust setup

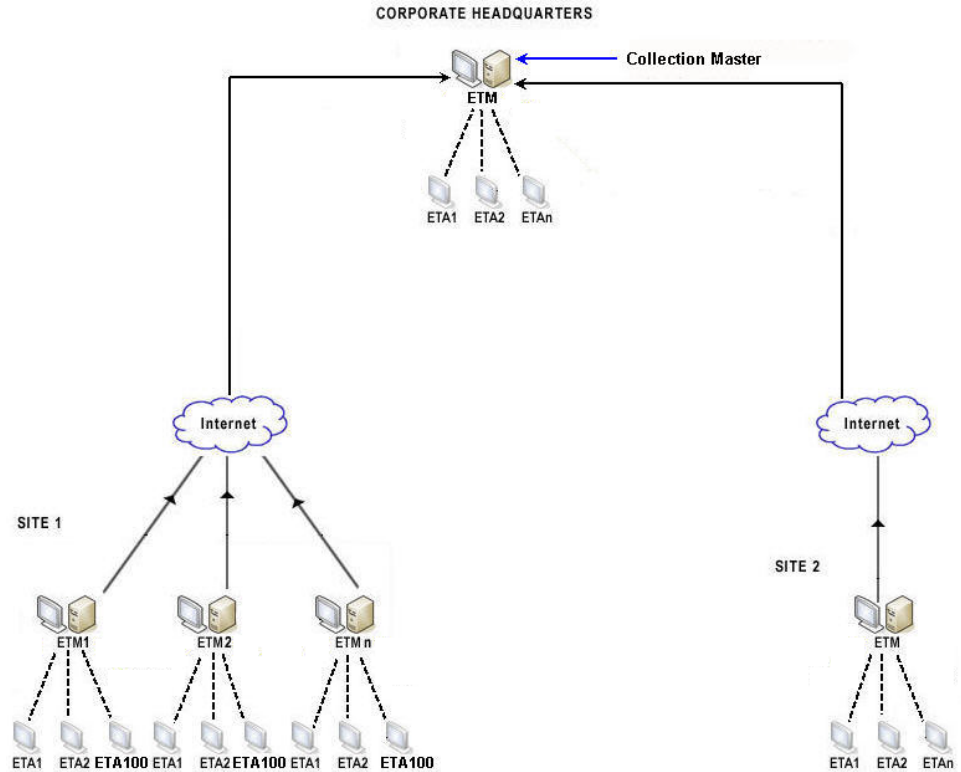
Real world scenarios

Figure 449
Scenario 1



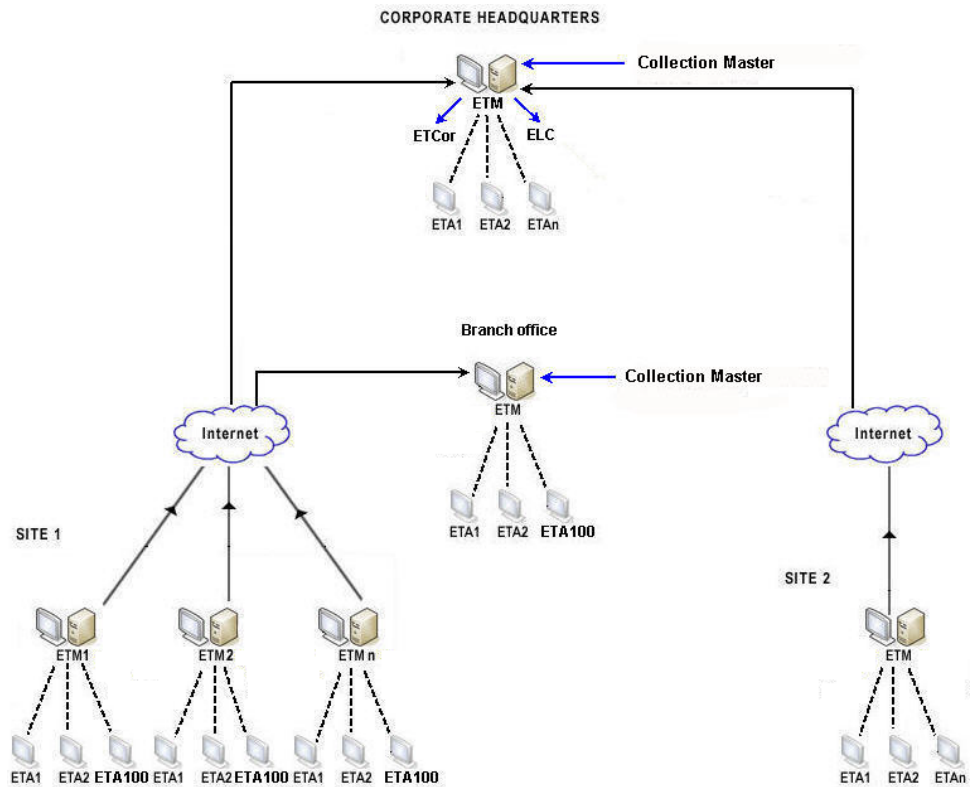
In the above-depicted scenario, all the Collection Points (clients) send their respective cab files periodically to the Collection Master (server) at the corporate headquarters.

Figure 450
Scenario 2



In this scenario, SITE 1 does exist physically in the same premises, which runs n number of EventTracker Managers. Each EventTracker Manager running Collection Point (client) will send the respective cab files to the Collection Master (server). The crux of the matter is that the Collection Master treats every individual EventTracker Manager running Collection Point (client) and the constellation of EventTracker Agents as different entities, no matter whether they exist in the same campus or on the same floor.

Figure 451
Scenario 3



The scenario above corroborates the statement that one Collection Point (client) could be configured to report up to five Collection Masters (servers).

Chapter 23

Collection Master

In this chapter, you will learn how to:

- [Start Collection Master](#)
- [View Collection Point Details](#)
- [Configure Collection Master listening port](#)
- [Delete CAB Files](#)
- [Delete Collection Point Details](#)

Starting Collection Master

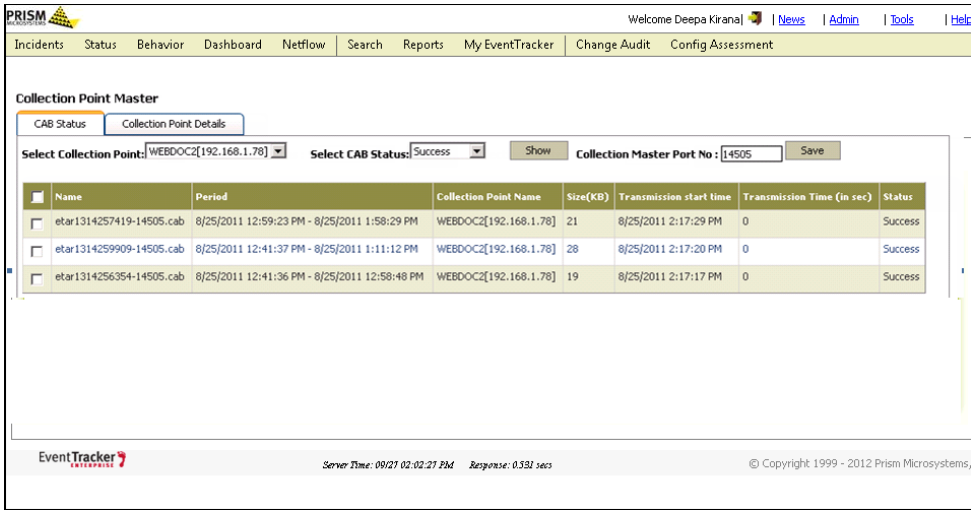
This option helps you open Collection Master Console.

To open Collection Master Console

- 1 Log on to EventTracker Enterprise.
- 2 Click the **Admin** hyperlink, and then click **Collection Master**.

EventTracker displays the Collection Point Master page.

Figure 452
Collection Master
CAB Status



'CAB status' tab is selected by default.

Table 134

Field	Description
Select Collection Point	Select the Collection Point from this drop-down list. All clients reporting to the Collection Master are listed in this drop-down list.
Select CAB status	Select the status of the cab files from this drop-down list and then click Show . Available options are Success , Failed and In Progress .
Collection Master Port No	By default, Collection Master and Collection Point communicate through port 14507. You can also change this port no. Type the port number and then click Save .

Table 135

Field	Description
Name	Name of the CAB file.
Period	Start and end time of events accommodated in the CAB file.
Collection Point Name	Name of the Collection Point that forwarded the CAB file.
Size (KB)	Size of the CAB file in kilobytes.
Transmission start time	Date and time when the Collection Point started to send the CAB file.
Transmission Time	Time taken to reach the destination.
Status	Transmission status of CAB files.

Viewing Collection Point Details

This option helps you view details of the Collection Points that are forwarding CAB files to the Collection Master.

To view Collection Point Details

- Click the **Collection Point Details** tab.

EventTracker displays the Collection Point Details page.

Figure 453
Collection Point
Details

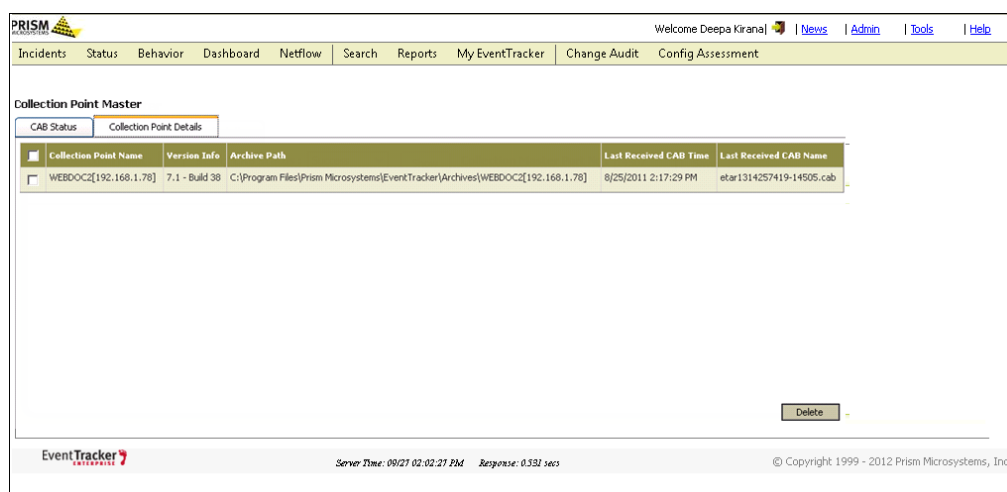


Table 136

Field	Description
Collection Point Name	Displays the name of the Collection Points that are reporting to the Collection Master.
Version Info	Displays the version of the Collection Points.
Archive Path	Displays the path of the folder where cab files of the respective Collection Points are stored at the Collection Master computer. Example: ...\\Program Files\\Prism Microsystems\\EventTracker\\Archives\\NEWYORK[192.168.1.38]
Last Received CAB Time	Date and Time when the Collection Master received the last CAB file.
Last Received CAB Name	Name of the last CAB file that is received from Collection Points.

Configuring Collection Master listening port

This option helps you configure listening port of the Collection Master. By default, EventTracker Collection Master and Collection Points communicate through port 14507. You can configure this port number from the Collection Master Console. If you configure a new port other than the default one, you have to configure at the Collection Points with the same port number for successful communication between the Collection Points and Collection Master.

To configure Collection Master listening port

- 1 Click the **CAB Status** tab.
 - 2 Type the port number in the **Collection Master Port No** field.
 - 3 Click **Save**.
-

Deleting CAB Files

This option helps you delete CAB files.

To delete CAB files

- 1 Click the **CAB Status** tab.
- 2 Select the checkbox on the title bar to select all CAB files.
(OR)
Select the checkbox against the CAB files.
- 3 Click **Delete**.

Deleting Collection Point Details

This option helps you delete Collection Point details.

To delete Collection Point details

- 1 Click the **Collection Point Details** tab.
- 2 Select the Collection Point.
- 3 Click **Delete**.

Note



When you delete details of a particular Collection Point, EventTracker will also delete their respective CAB files.

Chapter 24

Collection Point

In this chapter, you will learn how to:

- [View Collection Point Configuration](#)
- [Add Collection Masters](#)
- [Edit Collection Master Settings](#)
- [Delete Collection Master Settings](#)
- [View CAB Status](#)
- [Resend CAB Files](#)

Viewing Collection Point Configuration

This option helps you view Collection Point configuration.

To view Collection Point configuration

- 1 Log on to EventTracker Enterprise.
- 2 Click the **Admin** dropdown, and then click the **Collection Point**.

EventTracker displays the Collection Point page.

Figure 454
Collection Point
Configuration

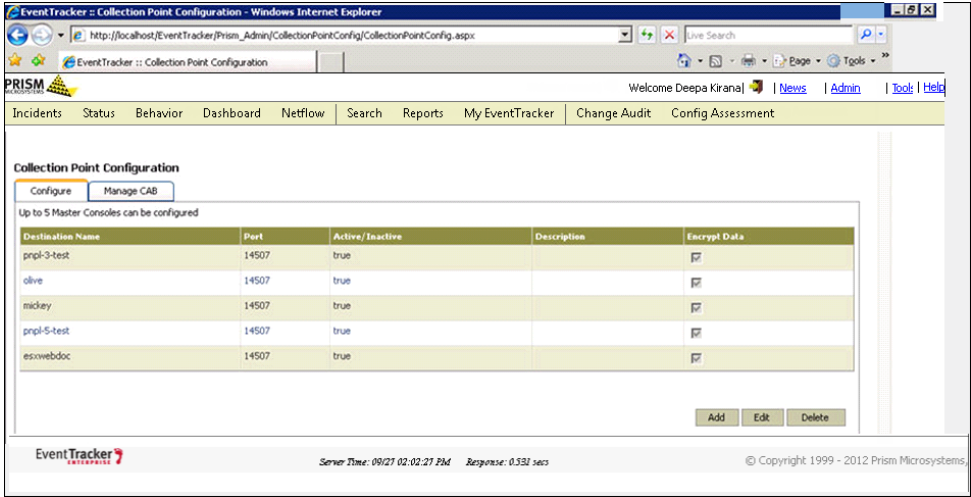


Table 137

Click	To
Add	Add new Collection master(s)/ manager(s).
Edit	Edit Collection master(s)/ manager(s) configuration settings.
Delete	Delete Collection master(s)/ manager(s) configuration settings.

Adding Collection Masters

This option helps you to add Collection Masters.

Every Collection Point can be configured to send CAB files simultaneously up to 5 Collection Masters. The Collection Master may exist in the same domain or in the trusted domain.

To configure Collection Masters

- 1 Click the **Configure** tab if not selected.

Table 138

Field	Description
Configure- Configured Collection Master(s) details are displayed on this page.	
Destination	Type the name / IP address of the Collection Master.
Port	Default port is 14507. You can modify the port number. Port numbers should be same on both the Collection Master and Collection Point.
Encrypt Data	Select an appropriate option to encrypt data. Go through the links provided in the Encryption section to know more about FIPS compliance.
Active	Select this checkbox to activate the Collection Master. Collection Point will not send CAB files to the Collection Master(s) that is Inactive.
Description	Type short description about the Collection Master.
Queue exist CABs	By default, EventTracker selects the Queue exist CABs checkbox and queues all existing CAB files. Clear this checkbox to queue only new CAB files.

- 2 Click **Add**.

Note

By default, EventTracker selects the **Active** checkbox. When you clear this checkbox, Collection Point will not send CAB files to the Collection Master that you have deactivated.

Collection Point can be configured to report up to 5 Collection Masters simultaneously. You can configure as many Collection Masters as possible and activate / deactivate them as the situations demand.

- 3 Enter/select appropriately in the relevant fields and then click **Add**.
-

Editing Collection Master Settings

This option helps you edit Collection Master Configuration settings.

To edit Collection Master Configuration settings

- 1 Click the **Configure** tab if not selected.
 - 2 Select the Collection Master, and then click **Edit**.
 - 3 Enter/select appropriate changes in the relevant fields, and then click **Save**.
-

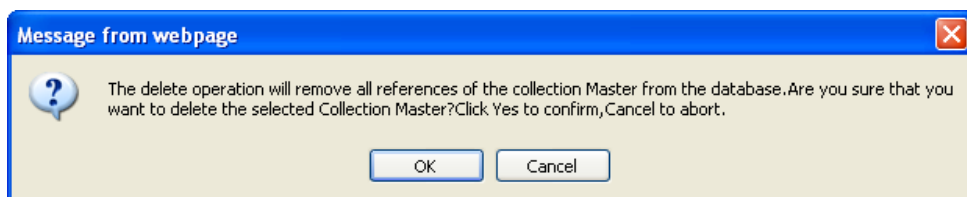
Deleting Collection Master Settings

This option helps you delete Collection Master Settings.

To delete Collection Master Settings

- 1 Click the **Configure** tab if not selected.
- 2 Select the Collection Master and then click **Delete**.
EventTracker displays the confirmation pop-up window.

Figure 455
Collection Point
Console
confirmation
message box



- 3 Click **Ok**.
EventTracker deletes the selected Collection Master Configuration settings.
-

Viewing CAB Status

This option helps you view status of the CAB files that are transferred and being transferred by the Collection Point to the Collection Master(s).

To view CAB status

- Click the **Manage CAB** tab.

Figure 456
CAB Status

Table 139

Field	Description
Select Destination	Select Destination from the drop-down list. All configured Collection Masters are listed in this drop-down list.
Select CAB Status	Select the status of the CAB files from this drop-down list and then click Show . Available options are Success, Failed, Do Not Send, In Progress and Queued .

Resending CAB Files

This option helps to resend CAB files.

To resend CAB files

- 1 Select the Collection Master from the **Select Destination** drop-down list.
- 2 Select the status from the **Select CAB Status** drop-down list.
- 3 Select the CAB files.
- 4 Click **Resend CAB**.

Collection Point resends the CAB file(s) to the destination(s).

Chapter 25

Auditing Changes

In this chapter, you will learn how to:

- [Set Dashboard Preferences](#)
- [View Summary of Change Details](#)
- [View Change Details – Change Details Console](#)
- [Authorize Unauthorized Changes](#)
- [View Access History](#)
- [View Additional Info on Files](#)
- [Enable O/S Auditing on Folders](#)
- [Enable O/S Auditing on Registry Keys](#)
- [Assess Changes](#)
- [Analyze Policy Comparison Results](#)
- [Schedule Change Assessment Policy Comparison](#)
- [Run Schedules On Demand](#)
- [Compare FDCC Policy](#)
- [View FDCC, DISA, and SCAP Scan Results](#)
- [Add Deviation](#)
- [Publish FDCC Report](#)
- [Create FDCC Report Bundle](#)

Why Should I Audit Changes?

Change auditing is the way to monitor voluntary and involuntary changes on your system and to make sure that your system has not been compromised. Ultimately, it helps to detect and recover from the most insidious of system compromises.

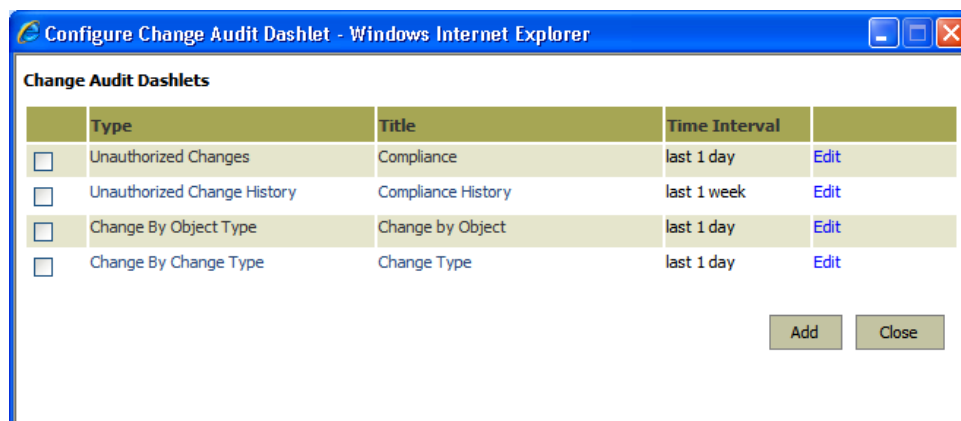
Change Audit Dashboard

Change Audit Dashboard allows you to add Dashlets to view Unauthorized Changes, Unauthorized Changes History, Change By Object Type, and Change By Change Type.

To view Change Audit Dashboard

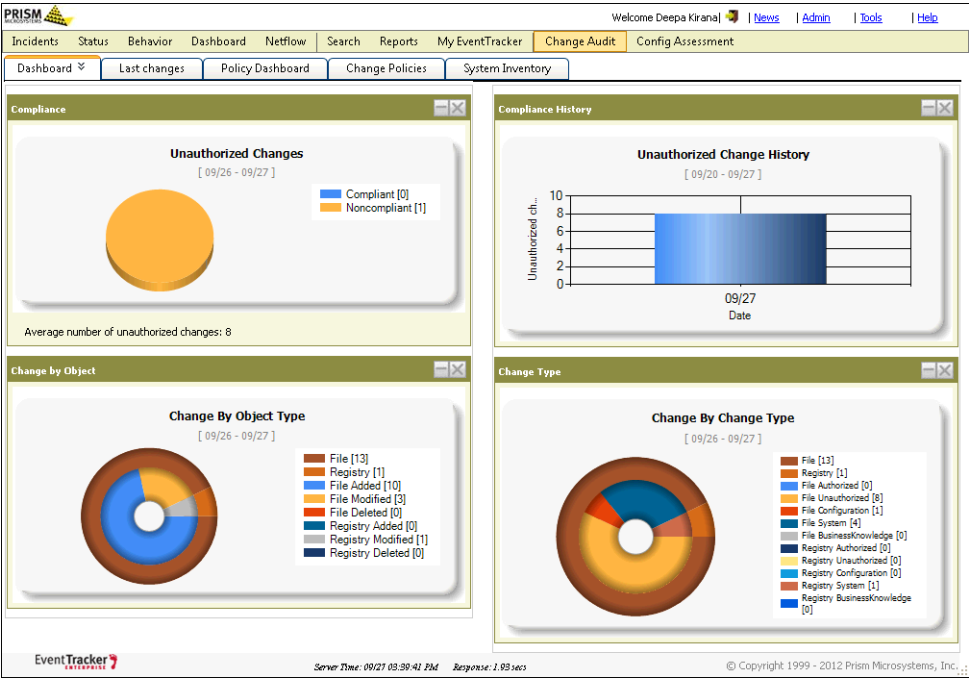
- 1 Log on to EventTracker Enterprise.
- 2 Click **Change Audit**.
(OR)
Move the mouse pointer over **Change Audit** and then click **Dashboard** on the menu.
EventTracker displays the Change Audit Dashboard.
- 3 Move the mouse pointer over Dashboard.
- 4 Click the **Customize** hyperlink.
EventTracker displays the Change Audit Dashlets pop-up window.

Figure 457
Change Audit
Dashlets



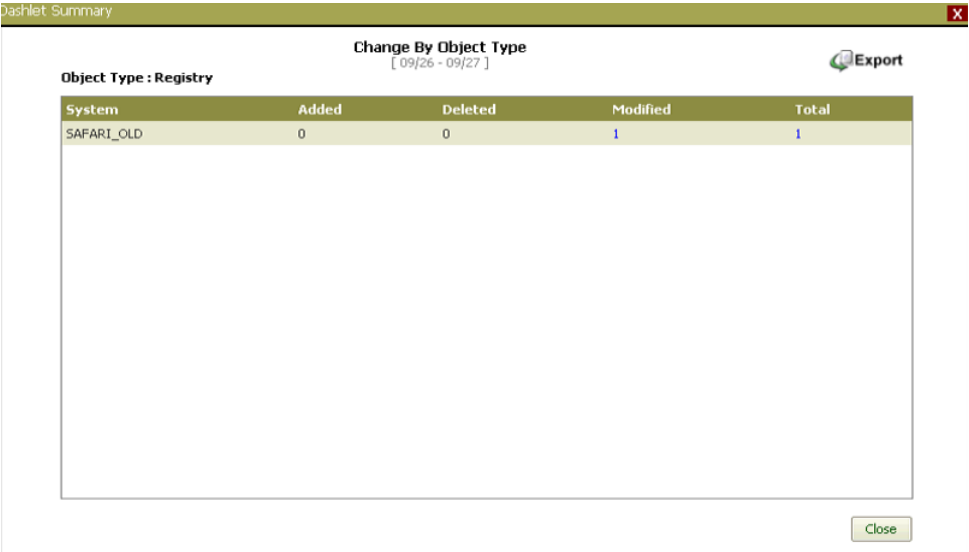
- 5 Click **Edit** to edit the Title or Time Interval settings, and then click **Update**.
- 6 Select the Dashlet(s) and then click **Add**.
EventTracker displays the Dashboard with newly added Dashlet(s).

Figure 458
Change Audit
Dashlets



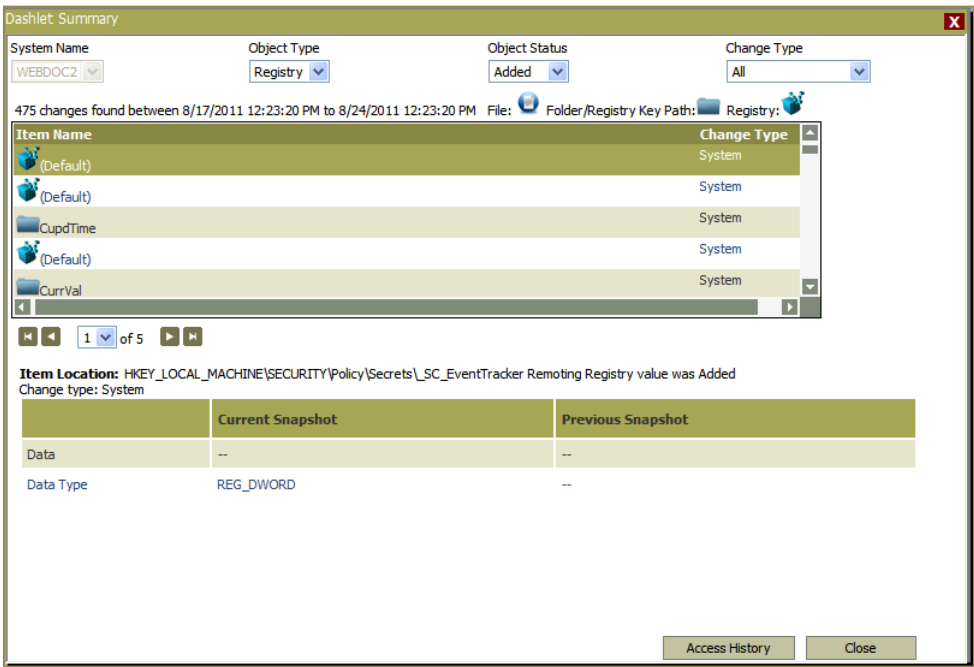
7 Click a graph or a legend to view respective Dashlet summary.

Figure 459
Dashlet Summary



8 Click a hyperlink to view respective change details.

Figure 460
Dashlet Summary



Viewing Last changes

Last changes tab displays the summary of snapshot comparison results.

To view the latest changes

- 1 Log on to EventTracker Enterprise.
 - 2 Click **Change Audit**.
 - 3 Click the **Last changes** tab.
- EventTracker displays the Last changes tab.

To view chart view summary of Change Type

By default, EventTracker displays chart view summary of Authorized, Unauthorized, Configuration, and Business Knowledge Change Types for all managed systems irrespective of the system groups.

'No data available' implies that no change has been detected for the default Change Types when the last snapshot was taken.

Figure 461
Change Policy
Dashboard

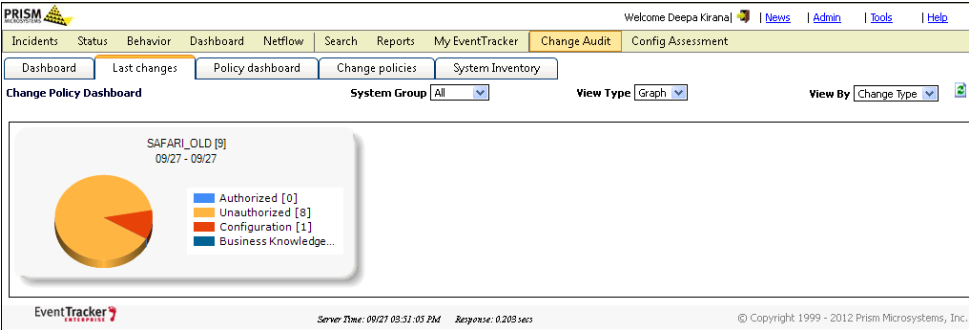


Table 140

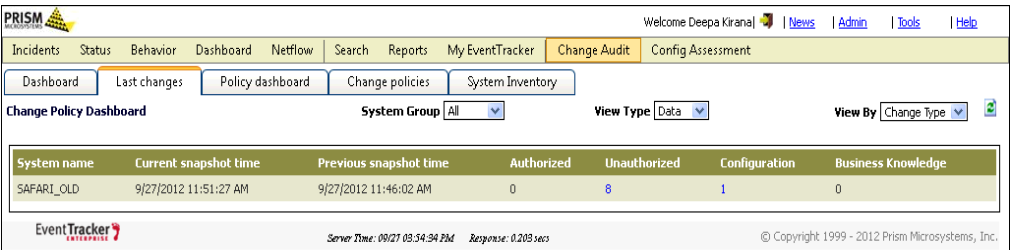
Change Type	Description
Authorized	Detected changes that can be matched with an approved change request.
Unauthorized	Detected changes that cannot be matched to an approved change request.
Configuration	Configuration audit helps to track all changes that have been made to a computer configuration, or to be able to restore the configuration of that computer back to a known valid restore point.
System	Detected changes in system files.
Business Knowledge	Is the concept in which an enterprise consciously and comprehensively gathers, organizes, shares, and analyzes its knowledge in terms of resources, documents, and people skills.

To view statistical data of Change Type/Object Type

1. In the **View Type** dropdown, click **Data**.
2. In the **View By** dropdown, click **Change Type/Object Type**.

EventTracker displays the statistical data of Change Type/Object Type.

Figure 462
Change Policy
Dashboard



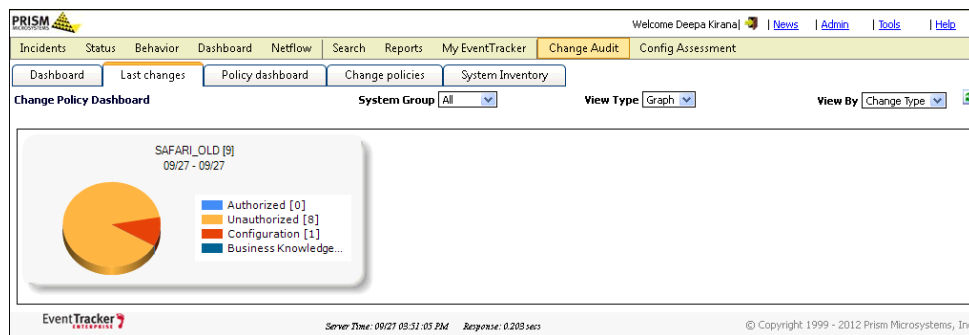
To view chart view summary of Change Type/Object Type

1. In the **View Type** dropdown, click the **Graph** option.

2. In the **View By** dropdown, click **Change Type/Object type**.

EventTracker displays the chart view summary of Change Type/Object Type.

Figure 463
Change Policy
Dashboard



Setting Dashboard Preferences

To set dashboard preferences

- 1 Double-click **Change Audit** on the EventTracker Control Panel.
EventTracker displays the Results Summary Console.
- 2 Click the **Tools** menu and then select the **Dashboard Preferences** option.
EventTracker displays the Dashboard Preferences window.

Figure 464
Dashboard
Preferences

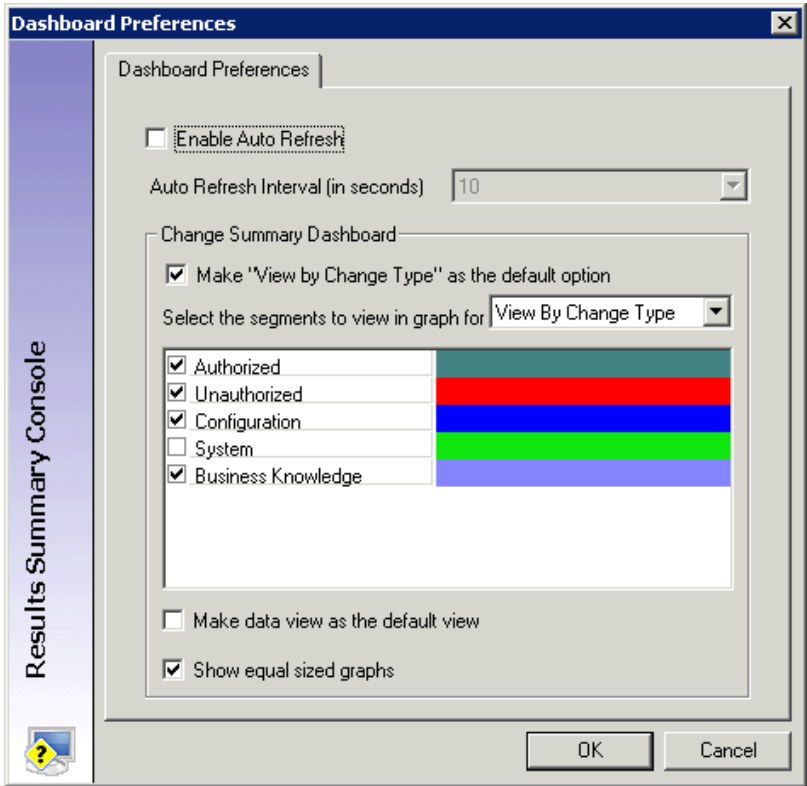
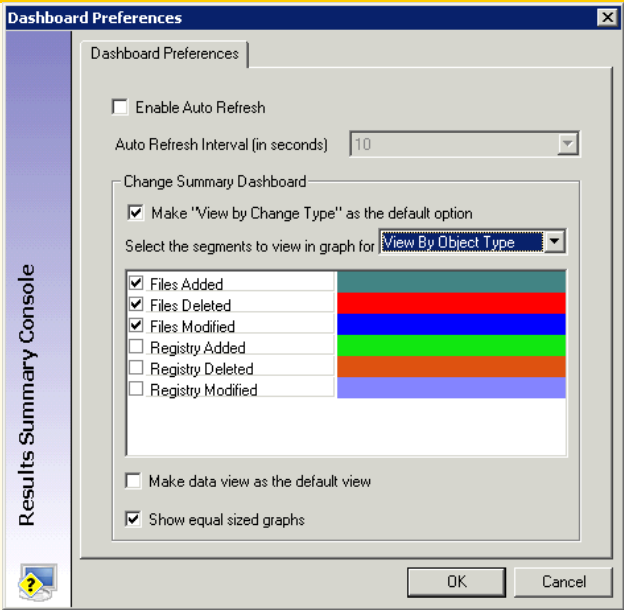


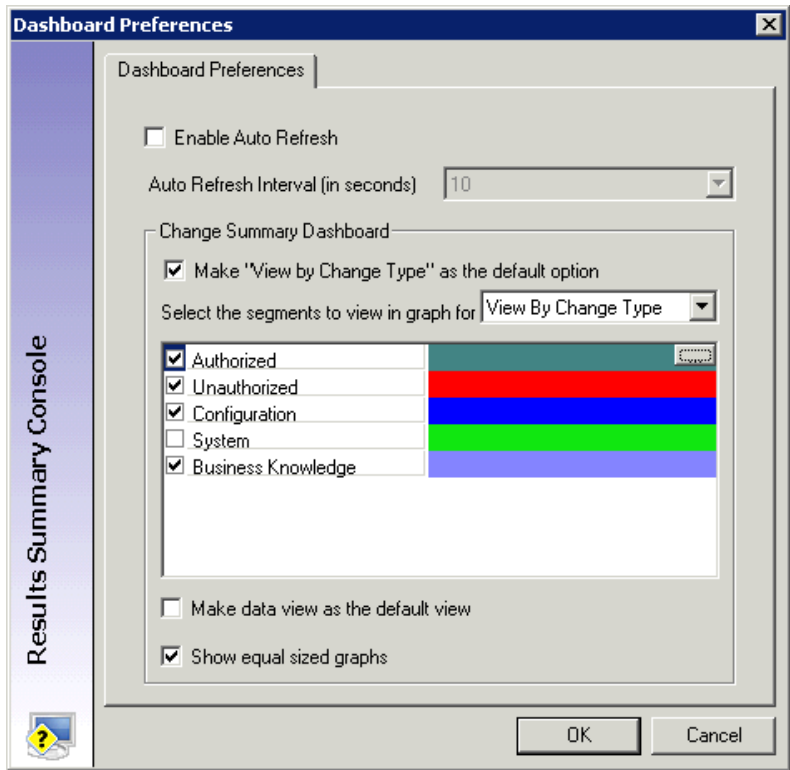
Table 141

Field	Description
Enable Auto Refresh	Select this checkbox if you prefer EventTracker to refresh the Results Summary Console automatically. EventTracker enables the 'Auto Refresh Interval [in seconds]' drop-down list. Set the interval for EventTracker to refresh the console.
Change Summary Dashboard	
Make "View by Change Type" as the default option	EventTracker selects this checkbox by default. Clear this checkbox if you prefer to view Object Type as default view.
Select the segments to view in graph for	EventTracker selects the 'View By Change Type' option by default and displays the related segments with respective color codes. You can select or clear the checkboxes against the respective segments.

Field	Description
	
Make data view as the default view	Select this checkbox if you prefer to view "Data View" by default. Otherwise, EventTracker displays the "Graph View" as default view.
Show equal sized graphs	EventTracker selects this checkbox by default. Clear this checkbox if prefer to view unequal sized graphs.

- Set the preferences and then click **OK**.
- To change the color of the preferred segment, click the color strip.
EventTracker displays the browse button.

Figure 465
Dashboard
Preferences



- 5 Click the browse button, EventTracker displays the color palette.
- 6 Select the color and then click **OK**.

Viewing Change Details

This option helps you view change details in the Change Details Console.

To view change details in the Change Details console

- 1 Click the **Last changes** tab.
- 2 Select the **View Type** option from the dropdown list.

View Type- Data

Figure 466
Last changes – View
by - Data

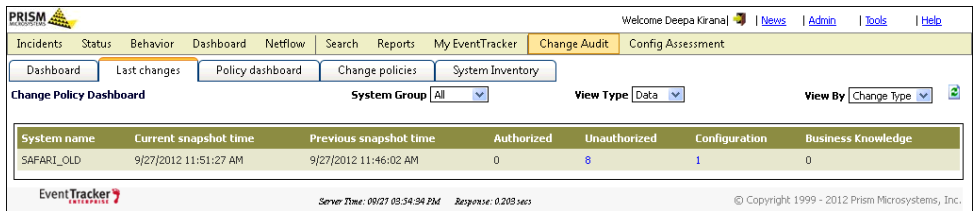
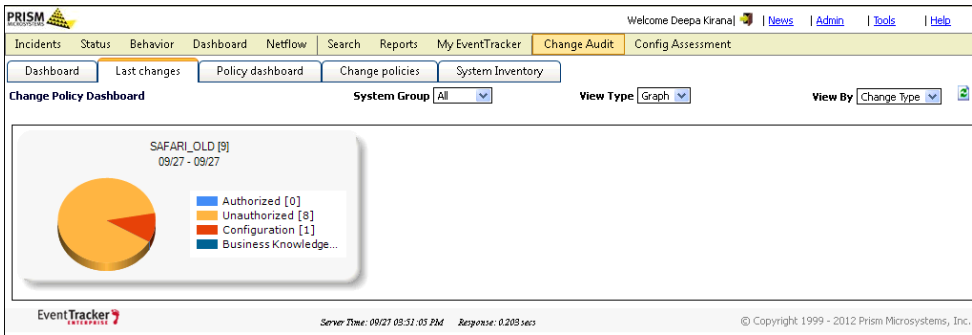


Figure 467
Last changes – View
by - Graph

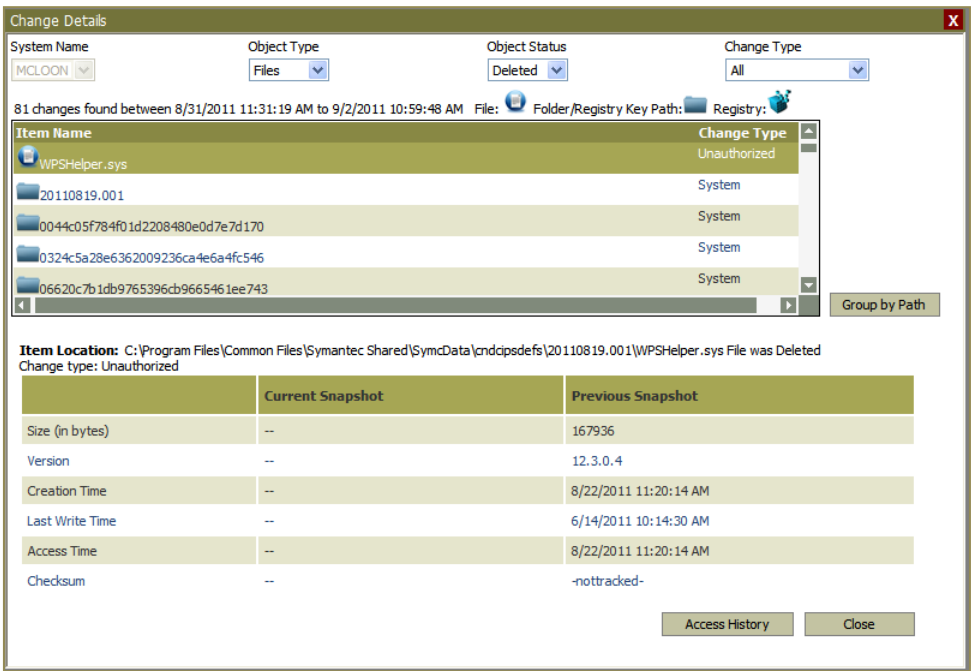
View Type - Graph



- 3 Click the hyperlink under the respective columns under **View Type- Data** or click on the pie section under **View Type- Graph**.

EventTracker displays the **Change Details** pop-up window.

Figure 468
Change Details



- 4 To further narrow down your search, select appropriately from the **Object Type**, **Object Status**, and **Change Type** drop-down lists.

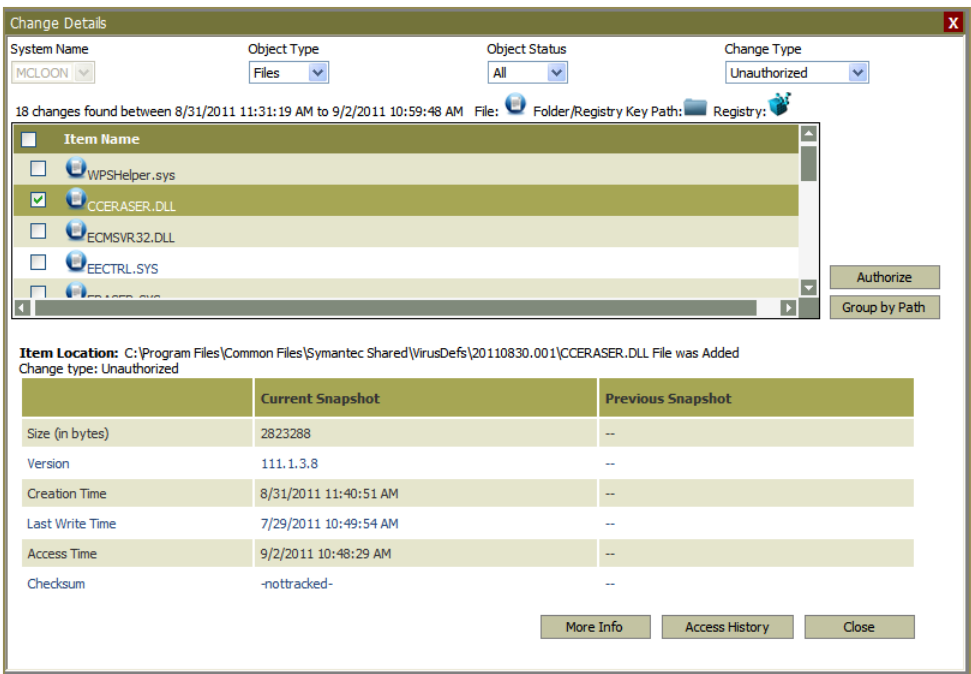
Authorizing Unauthorized Changes

To authorize unauthorized changes

- 1 Click the **Last changes** tab.
- 2 Click the hyperlink under the respective columns under **View Type- Data** or click on the pie section under **View Type- Graph**.

EventTracker displays the **Change Details** pop-up window.

- 3 Select the change type as **Unauthorized** from the Change type dropdown.



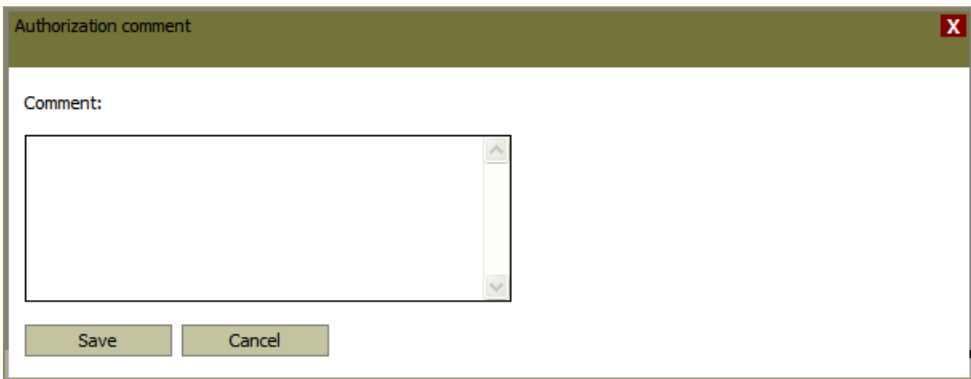
- 4 Select the checkbox against the item that you want to authorize.

You can also select/ unselect individual items by selecting or clearing the respective checkbox.

- 5 Click the **Authorize** button.

EventTracker displays the Authorization comment window.

Figure 469
Authorization
comment



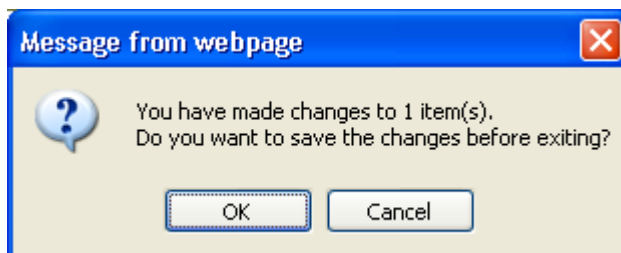
- 6 Type the reason why the selected item needs authorization in the **Authorization comment** field for future reference.

This field is not mandatory.

- 7 Click **Save**.

EventTracker displays the confirmation message pop-up window.

Figure 470
Confirmation
message box



- 8 Click **OK** to save changes.

EventTracker authorizes the selected item and removes from the unauthorized list.

You can also authorize items by grouping them based on a common location

- 9 Click **Group by Path** to view items by location.

EventTracker displays the Group by Path window.

Figure 471
Group by Path



- 10 If there are multiple paths displayed and you wish to select all paths, select the checkbox against **Path**, and then click the **Authorize** button to authorize all the items.

OR

To select individual path, select the checkbox for respective path, and then click the **Authorize** button.

Note



EventTracker enables Authorize button only for unauthorized items.

EventTracker displays the 'Authorize' button when changes to 'Unauthorized' items (*.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, and *.vxd) are detected.

EventTracker displays the 'More Info' button when new/modified/deleted DLLs and EXEs are detected.

Viewing Access History

This option helps you view access history of files, folders, and registry keys in a chronological order.

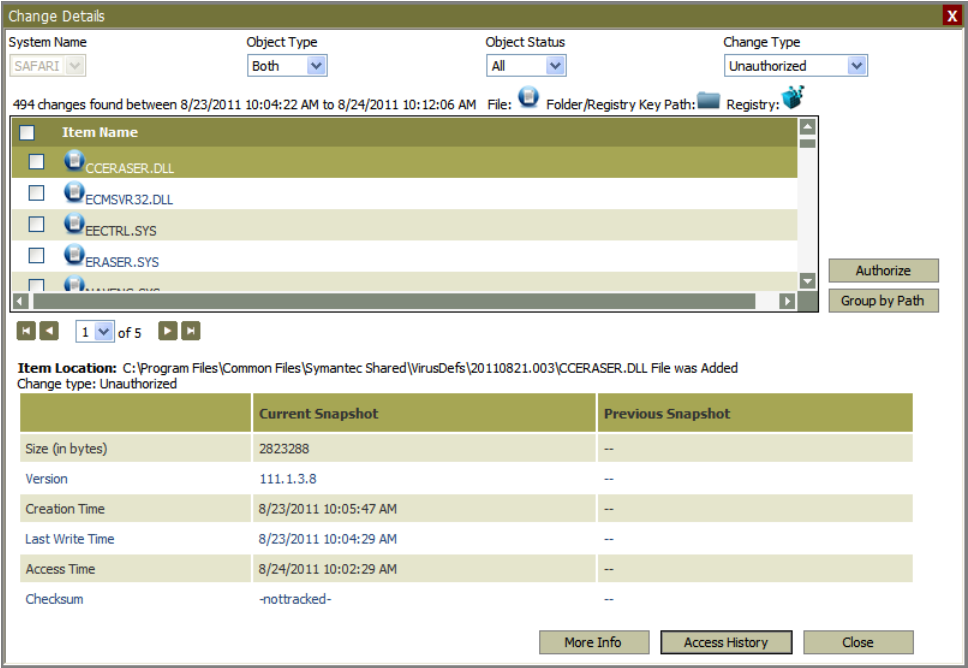
To view access history

Note



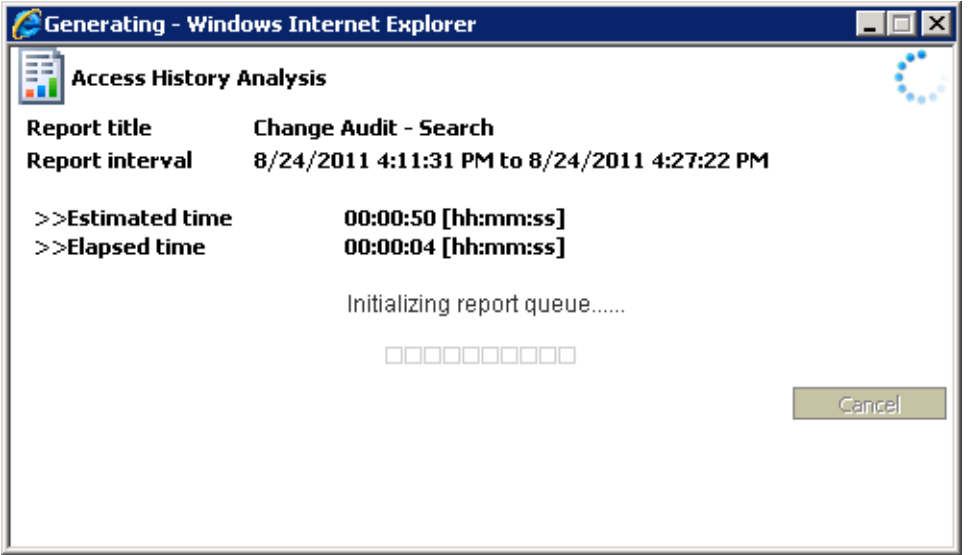
It is mandatory to enable Windows Object Access auditing on the target system prior to using this feature. For more details, refer the [Enabling O/S Auditing on Folder](#) section.

Figure 472
Change Details



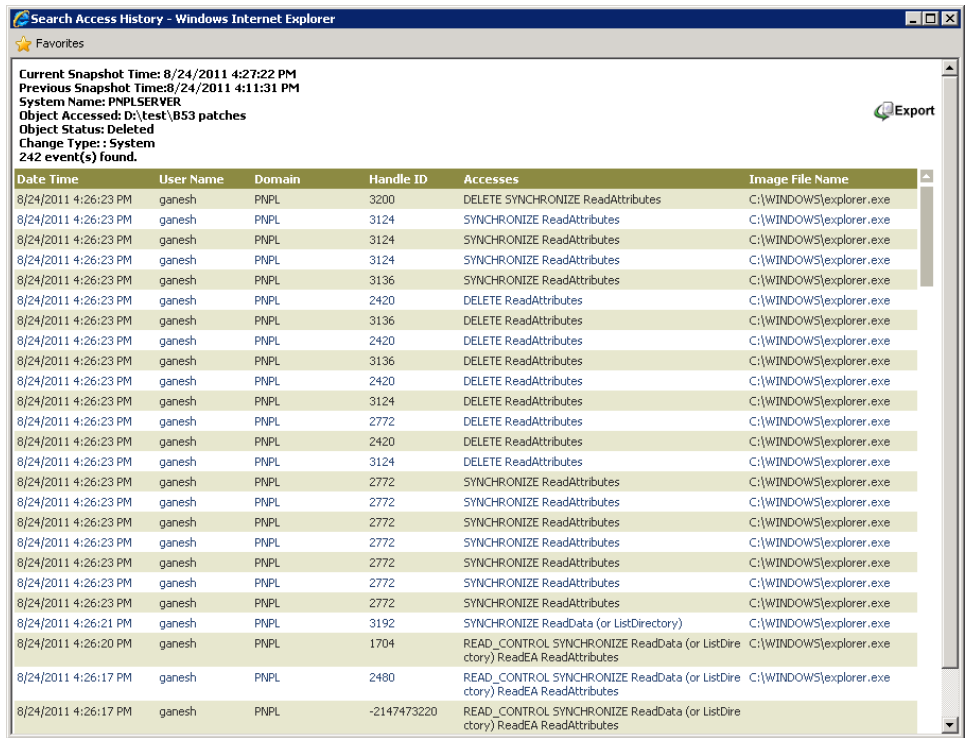
- 1 Select an item and then click **Access History**.
EventTracker displays the progress bar.

Figure 473
Change Details



EventTracker displays the access history of the selected item in a pop-up window.

Figure 474
Access History



Search Access History - Windows Internet Explorer

Current Snapshot Time: 8/24/2011 4:27:22 PM
Previous Snapshot Time: 8/24/2011 4:11:31 PM
System Name: PNPLSERVER
Object Accessed: D:\test\BS3 patches
Object Status: Deleted
Change Type: System
242 event(s) found.

Date Time	User Name	Domain	Handle ID	Accesses	Image File Name
8/24/2011 4:26:23 PM	ganesh	PNPL	3200	DELETE SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3124	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3124	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3124	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3136	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2420	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3136	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2420	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3136	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2420	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3124	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2772	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2420	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	3124	DELETE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2772	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2772	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2772	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2772	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:23 PM	ganesh	PNPL	2772	SYNCHRONIZE ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:21 PM	ganesh	PNPL	3192	SYNCHRONIZE ReadData (or ListDirectory)	C:\WINDOWS\explorer.exe
8/24/2011 4:26:20 PM	ganesh	PNPL	1704	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:17 PM	ganesh	PNPL	2480	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes	C:\WINDOWS\explorer.exe
8/24/2011 4:26:17 PM	ganesh	PNPL	-2147473220	READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes	C:\WINDOWS\explorer.exe

2 Click **Export** to export the report into Excel format.

Viewing Additional Info on Files

To view more info on files

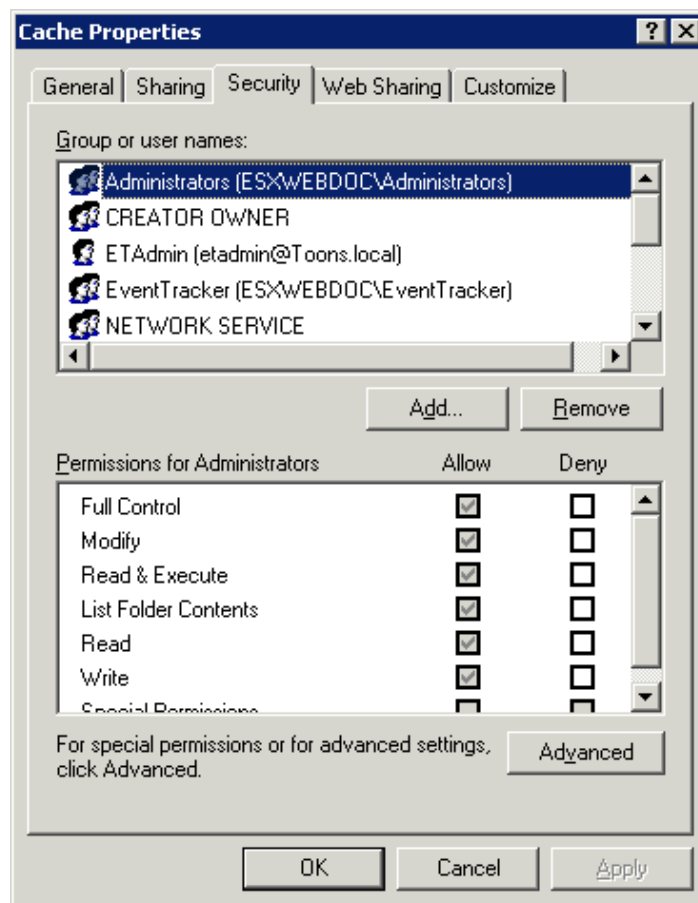
- Select an item and then click **More Info**.
EventTracker moves you through <http://www.processlibrary.com> Web site.

Enabling O/S Auditing on Folder(s)

To enable O/S auditing on folder(s)

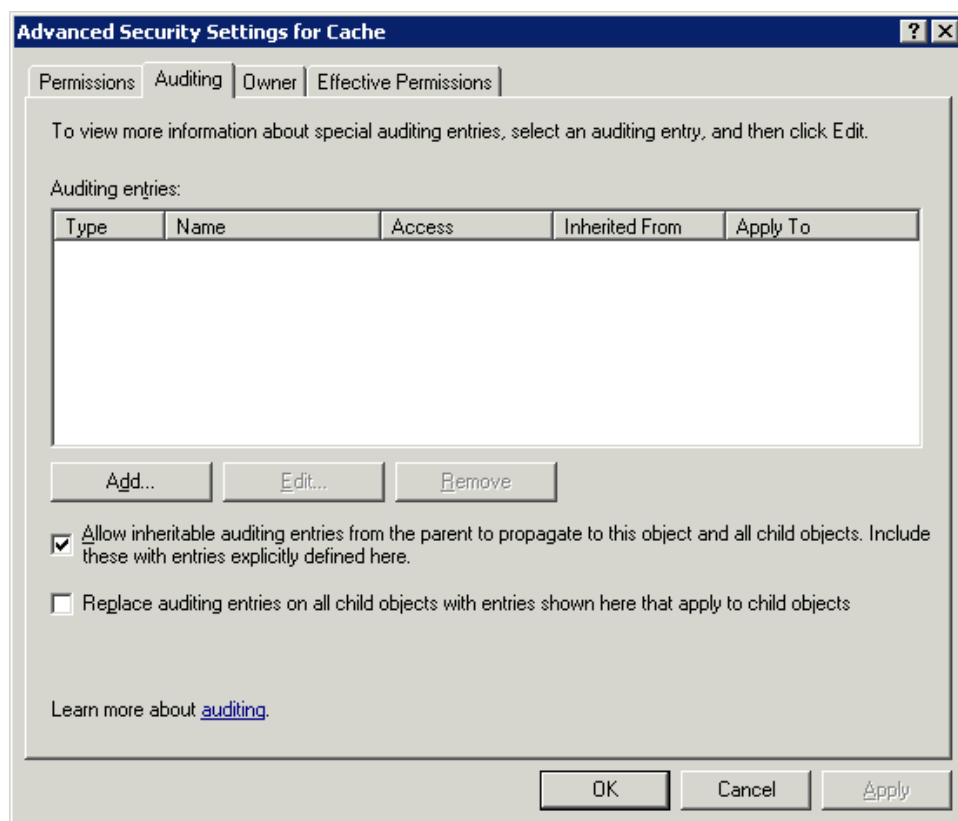
- 1 Right-click the folder that you want to audit. Example: [C:\Program Files\Prism Microsystems\EventTracker\Cache](#)
- 2 From the shortcut menu, choose **Properties**.
- 3 Click the **Security** tab on the Properties window.

Figure 475
Properties



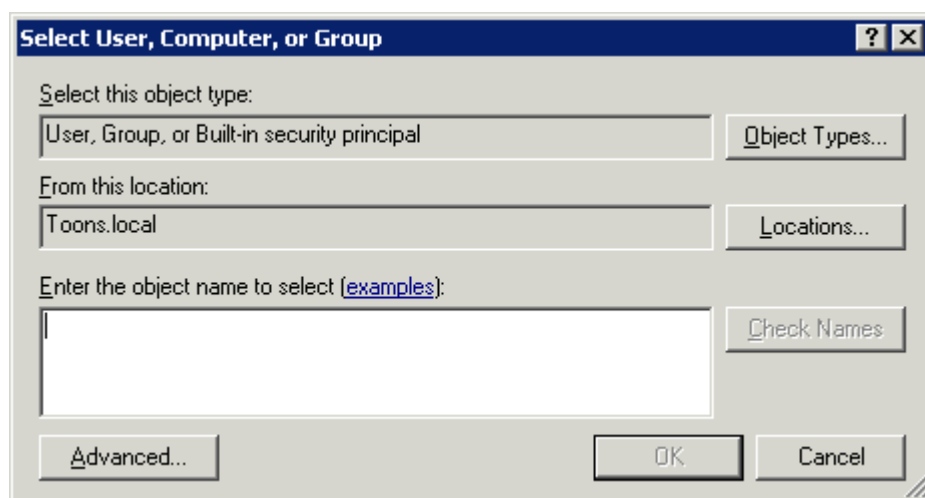
- 4 Click **Advanced**.
- 5 Click the **Auditing** tab on the Advanced Security Settings window.

Figure 476
Advanced Security
Settings



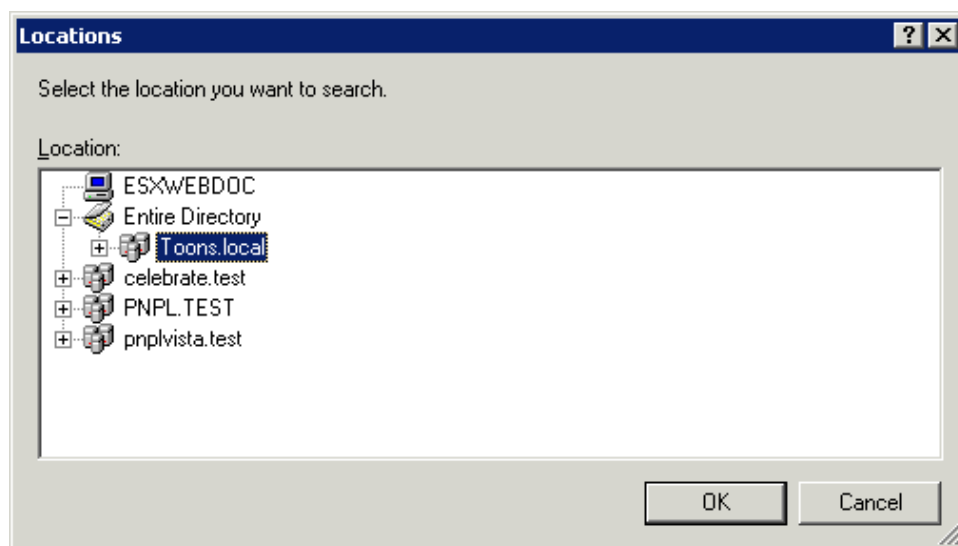
- 6 Click **Add**.
Select User, Computer, or Group window is displayed.

Figure 477
Select User,
Computer, or Group



- 7 Click **Locations**, to select the location from where you want to pick users.

Figure 478
Locations



- 8 Select the location from the **Locations** window and then click **OK**.
- 9 Enter the user name in the **Enter the object name to select** field. Example: Everyone
- 10 Click **Check Names**.

If the user name is valid, the user name is displayed in the Enter the object name to select field. Otherwise, an error message is displayed.

Figure 479
Select User,
Computer, or Group

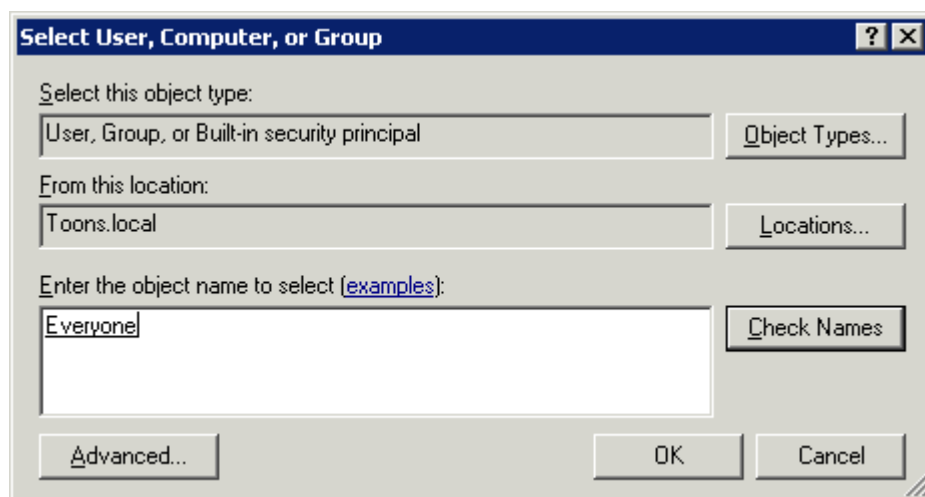
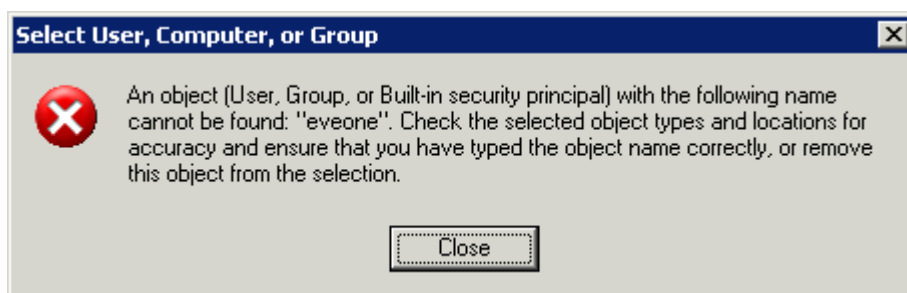


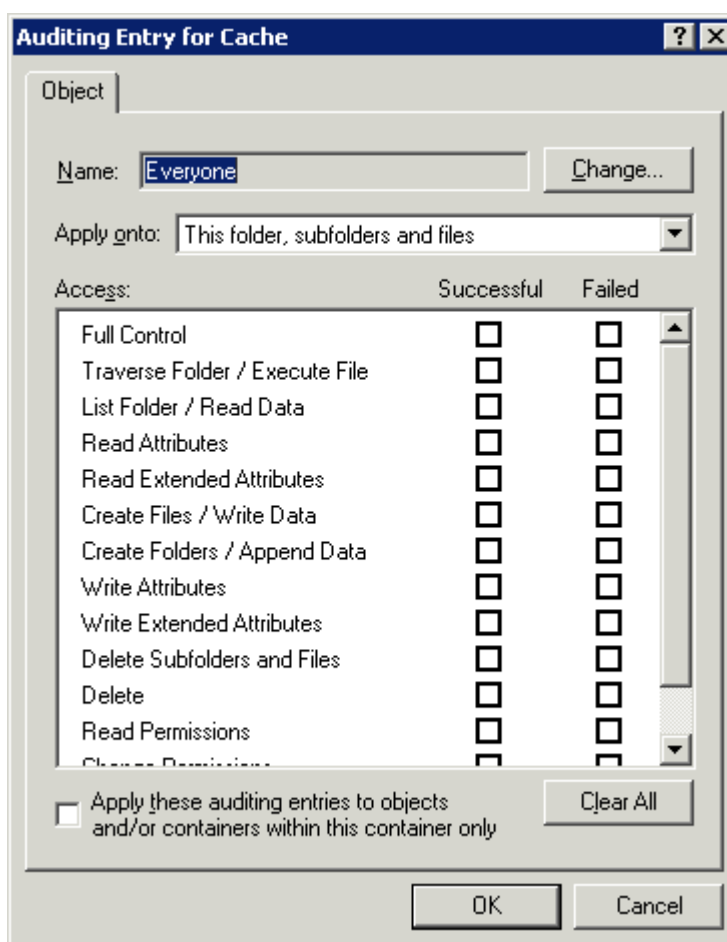
Figure 480



11 Click **OK**.

Auditing Entry for window is displayed.

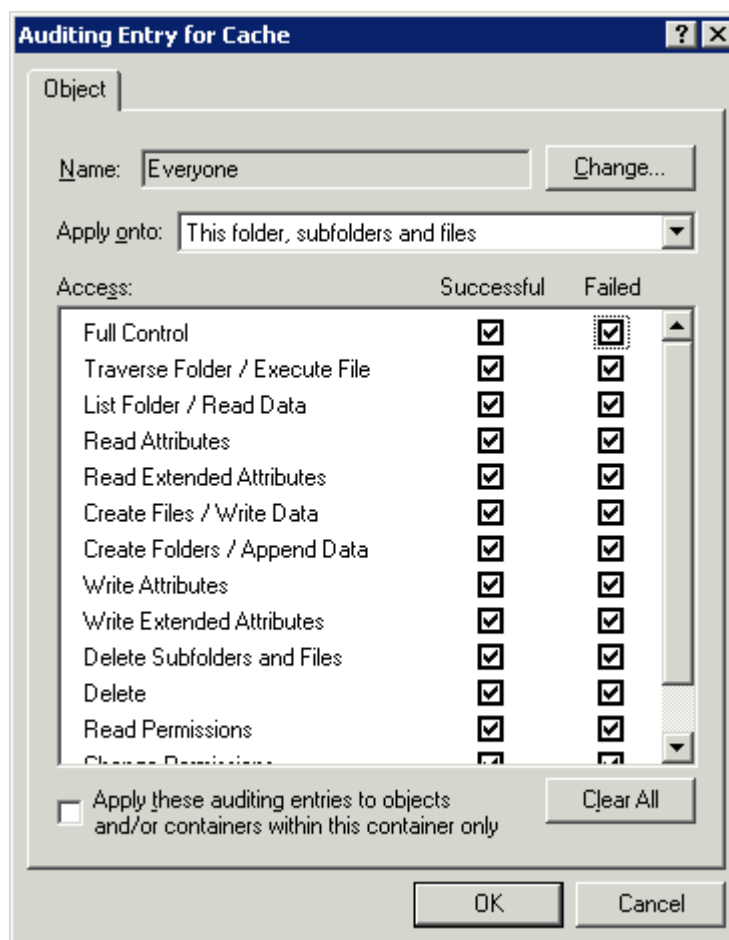
Figure 481
Auditing Entry



12 Select **Full Control** under **Successful** and **Failed**.

All other checkboxes are also selected automatically when you select **Full Control** checkbox.

Figure 482
Auditing Entry



Note

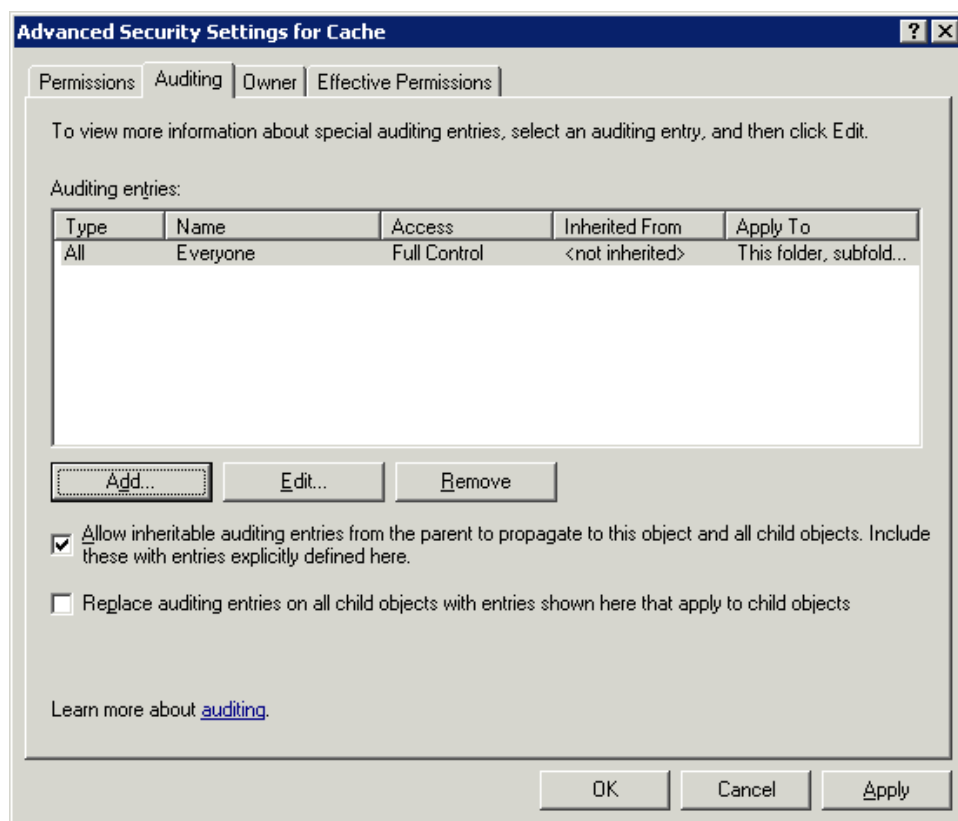


It is not mandatory to select the **Full Control** checkbox; rather, select the options as per your requirement.

13 Click **OK**.

Advanced Security Settings window is displayed with the newly added user.

Figure 483
Auditing Entry



- 14 Click **Apply**, and then click **OK**.
- 15 Click **OK** on the Properties window.

Note

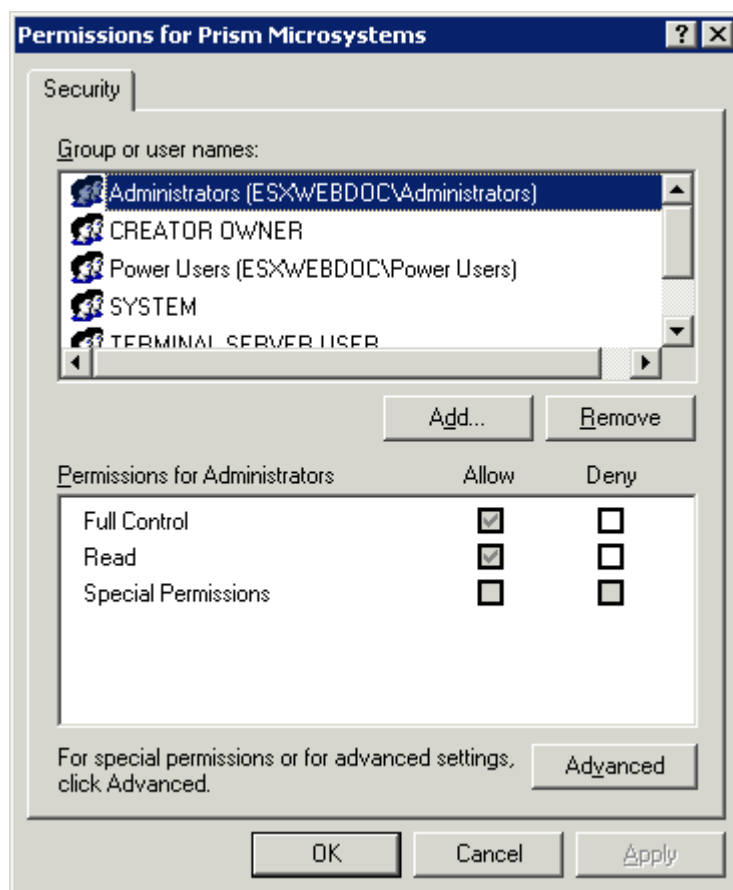
Similarly, you can enable auditing on files.

Enabling O/S Auditing on Registry Keys

To enable O/S auditing on registry keys

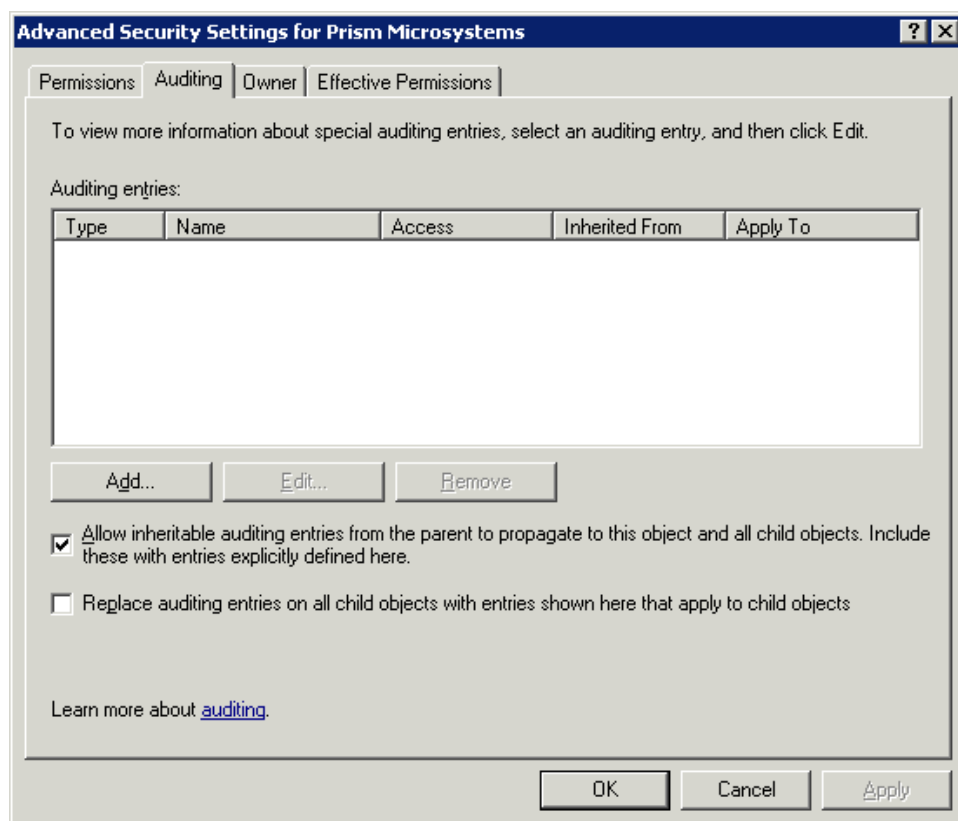
- 1 Open the **Registry** Editor.
- 2 Right-click the key that you want to audit.
- 3 From the shortcut menu, click **Permissions**.

Figure 484
Properties



- 4 Click **Advanced**.
- 5 Click the **Auditing** tab on the Advanced Security Settings window.

Figure 485
Properties



6 Add users as explained in the previous section.

Assessing the Changes

Change Assessment Dashboard displays the most recent results of on demand / scheduled policy comparison.

- Click the **Change policies** tab.

Figure 486
Change Assessment

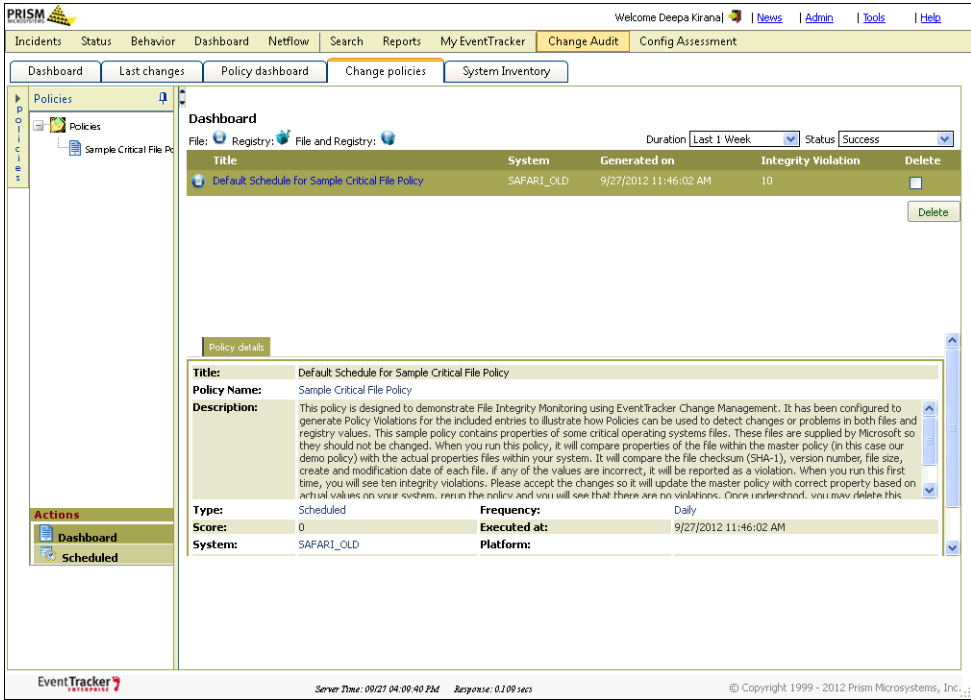


Table 142

Icon	Represents
	File changes found.
	Registry changes found.
	File and registry changes found.

Table 143

Field	Description
Duration	Select an option from this drop-down list to view policy comparison results for that period.
Status	Select an option from this drop-down list to further filter the policy comparison result. Success – policy comparison executed successfully against the monitored systems. Integrity Violations – policy comparison executed successfully against the monitored systems but integrity violations have been found. Exceptions – policy comparison execution failed.
Delete	Select the checkbox against the policy comparison result and then click this button.

Analyzing Policy Comparison Results

To analyze policy comparison results

- Click the title of the policy comparison schedule on the Dashboard.
EventTracker displays the Policy Comparison Results page.

Figure 487
Policy Comparison
Results window

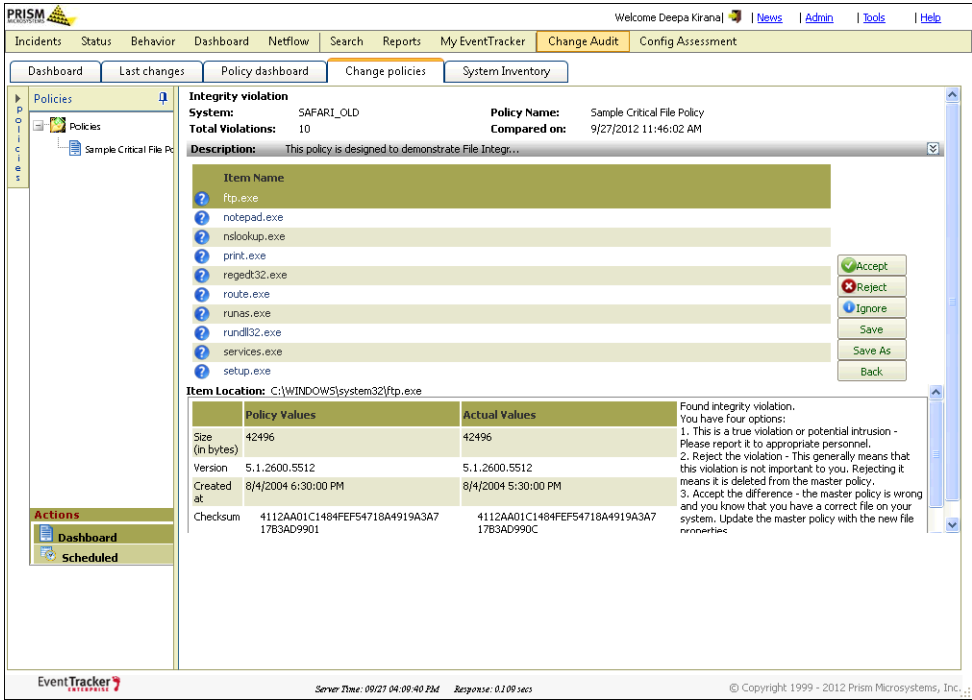





Table 144

Field	Description
System	Name of the target system where the policy is compared
Policy Name	Name of the policy compared on the target system.
Total Violations	Total number. of violations detected.
Compared on	Date and time when the policy was compared.
Description	Description of the policy.
Item Name	Name of the policy item.
Policy Values	Values of the policy item selected in the left pane when the policy was configured.
Actual Values	Actual Values of the policy item selected in the left pane after the policy comparison is done. This reflects any change in the value of the policy item.
Item Description	Description of the item selected in the left pane is displayed at

Field	Description
	the bottom of the right pane.

Field	Description
Accept	If changes are found for the selected item, you can update the master policy with the new value.
Reject	If you find an item to be irrelevant to the present context, you can select and remove that item from the master policy.
Ignore	When you generate a report, ignored items will not be considered for report generation. Note that these items are not removed from the master policy.
Save	Save the policy with changes if any, with the same name.
Save As	Save the policy with changes if any, with a different name.
Back	To go back to the Dashboard.

Table 145

Icon	Represents
	Fresh items.
	Items accepted.
	Items ignored.
	Items rejected.

For more information on creating Configuring Policies, refer http://www.prismmicrosys.com/WhatChanged%20Online%20Help/Creating_Configuration_Policies.htm

Scheduling Change Assessment

This option helps you schedule change assessment.

To schedule change assessment

- 1 Click **Scheduled** in the Actions pane.
- 2 Click **New Schedule** in the bottom pane.

Figure 488
Change Assessment

- 3 Type the title of the schedule in the **Title** field.
- 4 Select a policy from the **Policy Name** drop-down list.
Move the mouse pointer over **Tip** to view search hints.
- 5 Type the name of the system(s) in the **Search system(s)** field and then click the search icon.
EventTracker displays the system group of the systems searched.
- 6 Select the system(s).
- 7 Click **Show All** to view all managed systems and system groups.
(OR)
Select system(s)/system group(s) from the **Systems** list.
- 8 Set date and time, when to run the schedule.
- 9 Select an option from the **Frequency** drop-down list, how often should the policy be run.
EventTracker enables the **Week Day** drop-down list only when you select the Weekly option from the Frequency drop-down list.
- 10 Click **Save**.

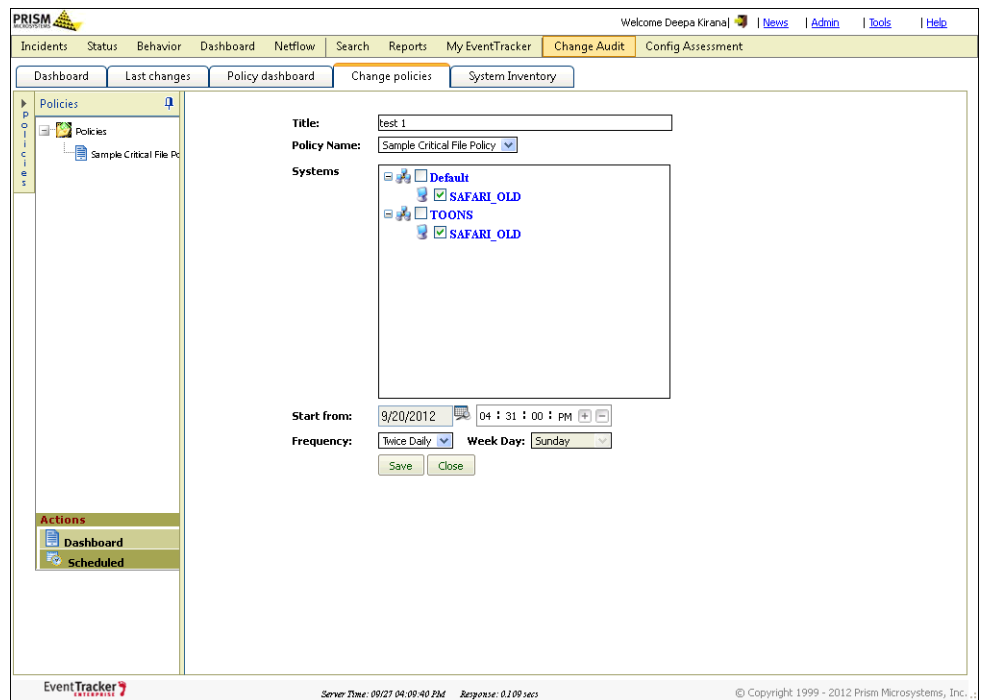
Editing Change Assessment Schedules

This option helps you edit Change Assessment schedules.

To edit Change Assessment schedules

- 1 Select a scheduled policy in the bottom pane.
- 2 Click **Edit**.

Figure 489
Change Assessment



- 3 Make appropriate changes in the relevant fields.
- 4 Click **Save**.

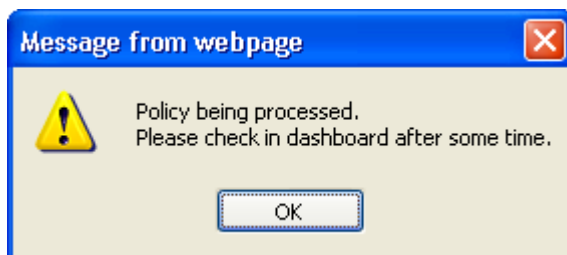
Running Schedules On Demand

This option helps you run schedules on demand.

To run schedules on demand

- 1 Select a scheduled policy in the bottom pane.
- 2 Click **Run Now**.
EventTracker displays the message box with appropriate message.

Figure 490
Information
message box



Deleting Scheduled policies

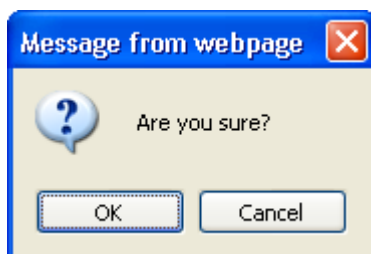
This option helps you delete schedules.

To delete schedules

- 1 Select a scheduled policy in the bottom pane.
- 2 Click **Delete**.

EventTracker displays the confirmation message box.

Figure 491
Confirmation
message box



- 3 Click **OK** to delete the schedule.

Viewing Policy Dashboard

Policy Dashboards helps to add Dashlets to view the compliance status of systems against which the Policies were compared.

To view Policy Dashboard

- 1 Click the **Policy Dashboard** tab.
- 2 Move the mouse pointer over Policy Dashboard.
- 3 Click the **Configure** hyperlink.
EventTracker displays the Configure Benchmark Dashlets pop-up window.
- 4 Type a comprehensible name in the **Display Name** field.

- 5 Select a policy from the **Policy Name** field.
EventTracker displays the Configure Benchmark Dashlets pop-up window with Schedule details of the selected Policy.
- 6 Click the checkbox to select the Schedule(s).

Figure 492
Configure
Benchmark Dashlets

Configure Benchmark Dashlet				
Schedules				
	Title	Frequency	Scheduled at	System
<input type="checkbox"/>	Default Schedule for Sample Critical File Policy	Daily	8/25/2011 11:24:00 AM	1. SAFARI

- 7 Click the **Configure** button.

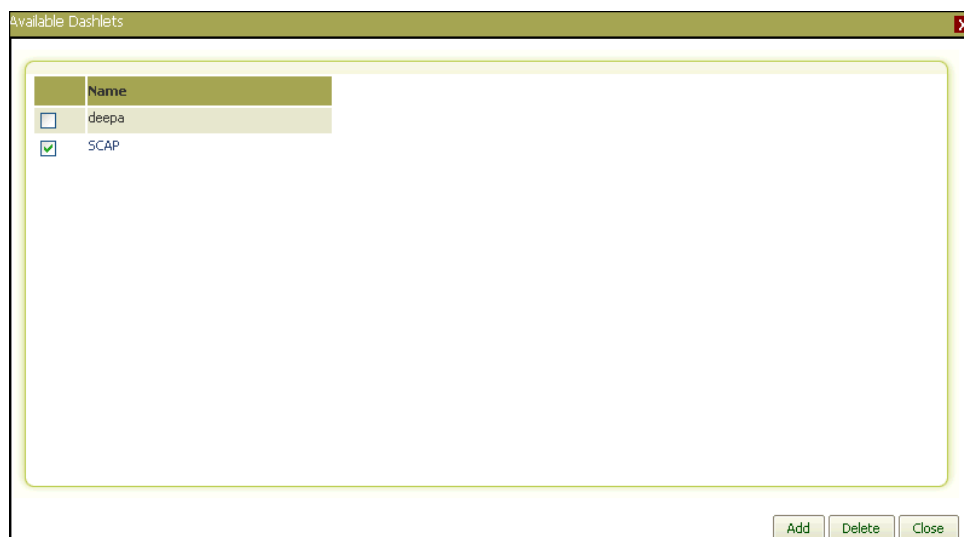
Customizing the Policies Dashboard

This option helps to customize the dashboard with configure Dashlets.

To customize the Policies Dashboard

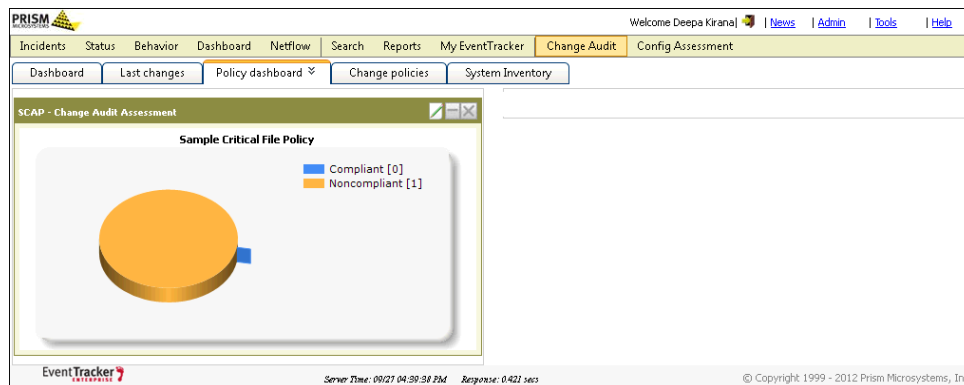
- 1 Move the mouse pointer over **Policies Dashboard**.
- 2 Click the **Customize** hyperlink.
EventTracker displays the Available Dashlets pop-up window.

Figure 493
Available Dashlets



- 3 Click the checkbox to select the Dashlet(s), and then click **Add**.
EventTracker adds the Dashlet(s) to the Dashboard.

Figure 494
Change Audit
Assessment



OR

Click the checkbox to select the Dashlet(s), and then click **Delete**.
EventTracker deletes the dashlet(s).

- 4 Click a pie or a legend to view respective system details.
EventTracker displays the System Details Pop-up window.

Figure 495
System Details

View	System	File Changes	Registry Changes	Assessment Time
View	SAFARI	10	0	8/25/2011 11:28:52 AM

5 Click the **View** hyperlink to view Change Audit Assessment Details.

Figure 496
Change Audit
Assessment Details

Integrity violation
System: SAFARI **Policy Name:** Sample Critical File Policy
Total Violations: 10 **Compared on:** 8/25/2011 11:28:52 AM
Description: This policy is designed to demonstrate File Integr...

Item Name

- ftp.exe
- notepad.exe
- nslookup.exe
- print.exe
- regedt32.exe
- route.exe
- runas.exe
- rundll32.exe
- services.exe

Item Location: C:\WINDOWS\system32\ftp.exe

	Policy Values	Actual Values
Size (in bytes)	42496	42496
Version	5.1.2600.5512	5.1.2600.5512
Created at	8/4/2004 6:30:00 PM	8/4/2004 5:30:00 PM
Checksum	4112AA01C1484FEF54718A4919A3A717B3AD9901	4112AA01C1484FEF54718A4919A3A717B3AD990C

Found integrity violation. You have four options:
1. This is a true violation or potential intrusion - Please report it to appropriate personnel.
2. Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy.

EventTracker Inventory Manager

EventTracker Inventory is an automated asset management tool, which scans all Change Audit, managed computers, and displays them in an easy accessible web and legacy interface.

Software inventory: To track and audit software installed on Change Audit managed computers.

To view applications and updates

- 1 Double-click **Change Audit** on the EventTracker Control Panel.

EventTracker displays the Results Summary Console.

Note



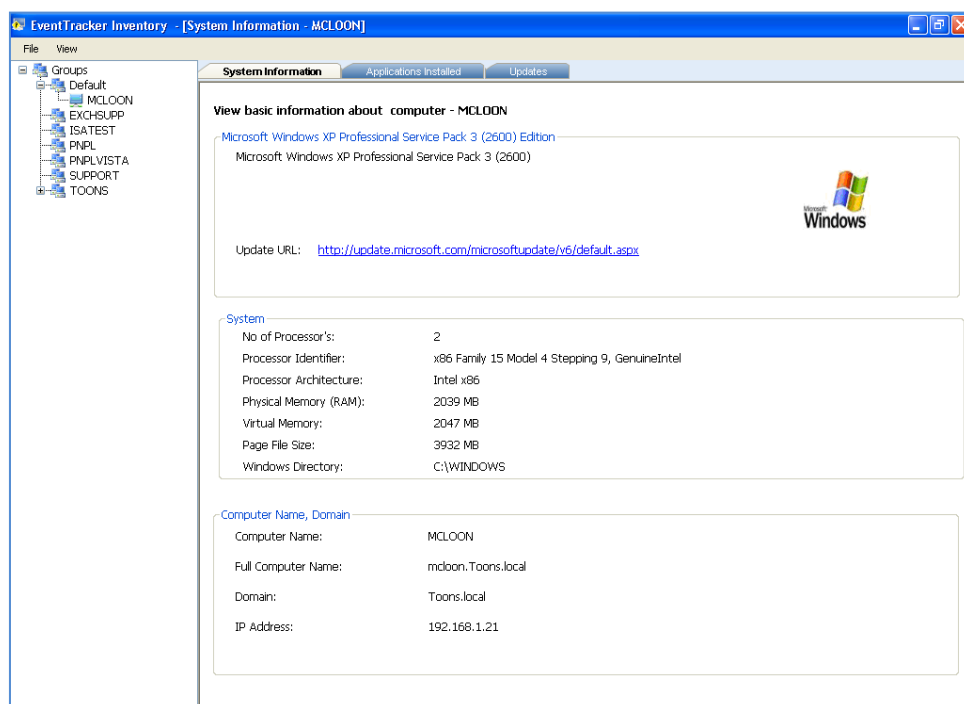
You can also access the Inventory Manager by clicking the **System Inventory** tab on the Change Audit page on the web interface.

- 2 Click the **Tools** menu and then select the **Inventory Manager** option.

EventTracker displays the EventTracker Inventory Manager with enterprise system groups and Change Audit managed systems under their respective groups.

By default, Inventory Manager displays system details of EventTracker Manager System.

Figure 497
Inventory Manager



- 3 Expand the system group and select the system that you want to view details.
- 4 Click the **View** menu and select the **Applications Installed** option.
(OR)

Click the **Applications Installed** tab.

Inventory Manager displays the itemized list of applications installed on the selected system.

Figure 498
Applications
Installed

EventTracker Inventory - [Application Installed - MCL00N]

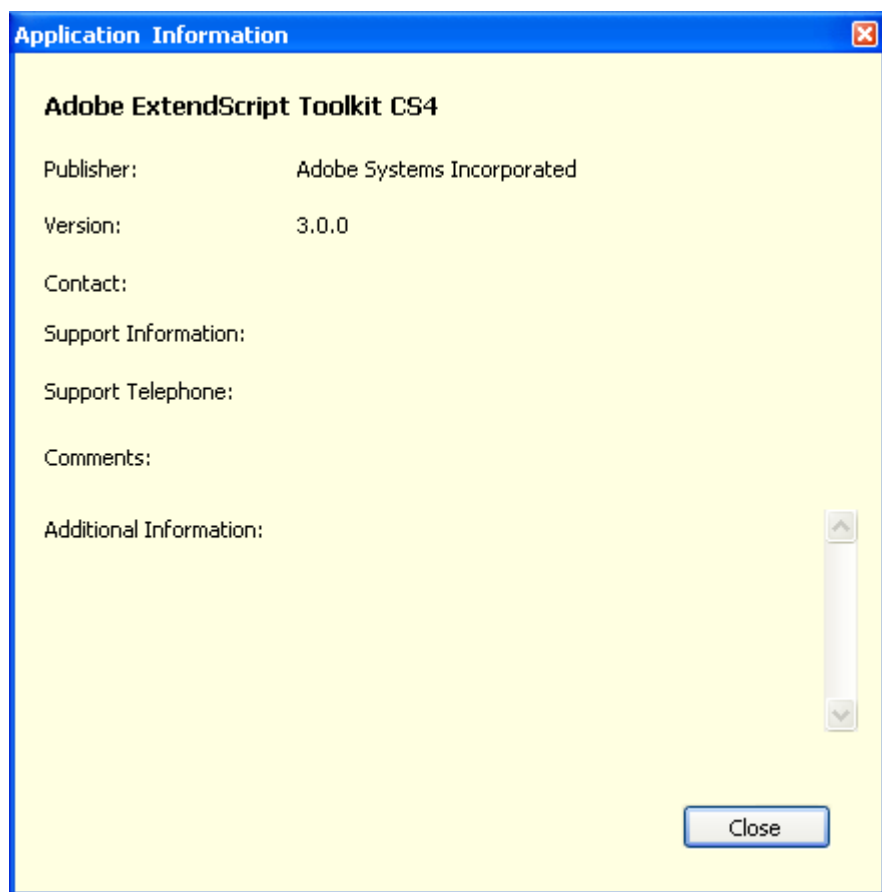
System Information Applications Installed Updates

Currently Installed Programs - MCL00N

Application Name	Size	Install Date	Version	Size	28MB
Installation Date					
Adobe ExtendScript Toolkit CS4					
Click here to see details					
Adobe Flash Player 10 ActiveX	8MB		10.3.181.34		
Adobe PDF Creation Add-On 9		12-APR-2011	9.0.0		
Adobe Reader 8.3.0	88MB	20-JUL-2011	8.3.0		
Adobe RoboHelp 8.0.2			8.0.2		
Bing Bar			5.0.1363.0		
EventTracker	368MB	25-AUG-2011	7.2		
EventTracker KB Search Bar	0MB	11-MAY-2011	1.0.2		
Intel(R) Graphics Media Accelerator Dr...			6.14.10.4436		
IP Messenger for Win					
Microsoft .NET Framework 2.0 Service...	560MB	12-APR-2011	2.2.30729		
Microsoft .NET Framework 3.0 Service...	169MB	12-APR-2011	3.2.30729		
Microsoft .NET Framework 3.5 SP1					
Microsoft Office Professional 2007			12.0.4518.1014		
Microsoft Silverlight	15MB	17-JUN-2011	3.0.40818.0		
Microsoft SQL Server 2005					
Microsoft SQL Server 2008 R2 Native ...	4MB	25-AUG-2011	10.50.1600.1		
Microsoft SQL Server 2008 R2 Setup [...]	37MB	22-AUG-2011	10.50.1600.1		
Microsoft SQL Server 2008 Setup Sup...	26MB	25-AUG-2011	10.1.2731.0		
Microsoft SQL Server Browser	8MB	25-AUG-2011	10.50.1600.1		
Microsoft SQL Server Management St...	116MB	13-JUL-2011	9.00.3042.00		
Microsoft SQL Server Native Client	4MB	11-JUL-2011	9.00.3042.00		
Microsoft SQL Server Setup Support F...	21MB	11-JUL-2011	9.00.3042.00		
Microsoft SQL Server VSS Writer	6MB	25-AUG-2011	10.50.1600.1		
Mozilla Firefox (3.6.8)			3.6.8 (en-GB)		
MSXML 6.0 Parser	1MB	11-JUL-2011	6.10.1129.0		
REALTEK GbE & FE Ethernet PCI NIC...		12-APR-2011	1.02.0000		

- 5 Click the ‘here’ hyperlink to view details.
Inventory Manager displays the details in a pop-up window.

Figure 499
Application
Information



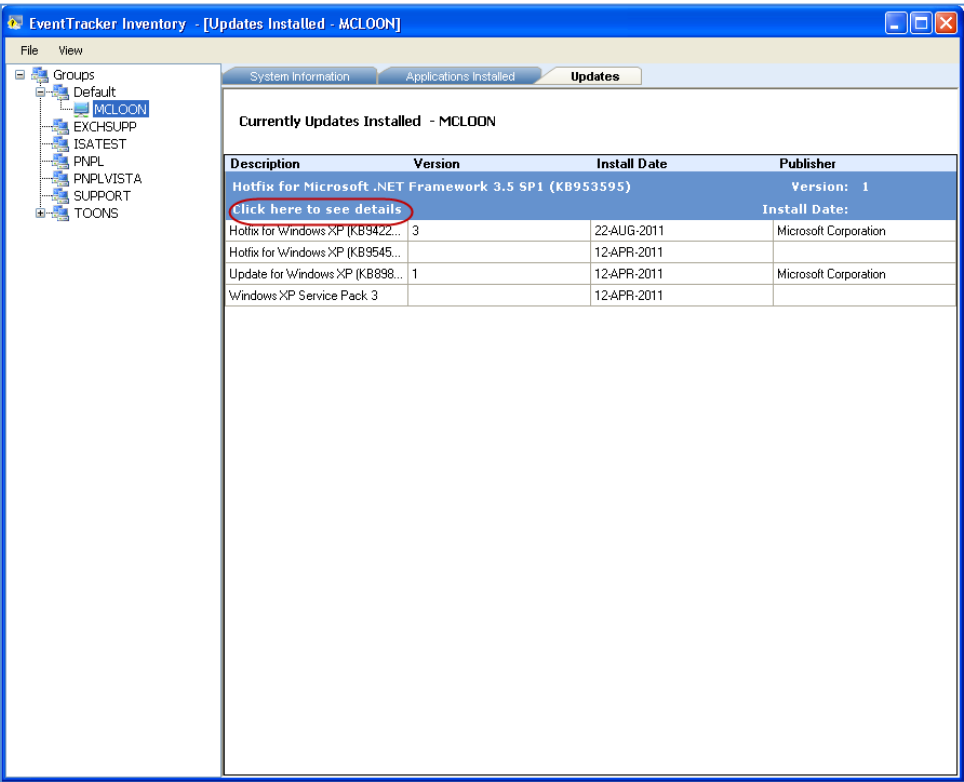
- 6 Click the **View** menu and select the **Updates** option to view hotfixes, patches, and updates.

(OR)

Click the **Updates** tab.

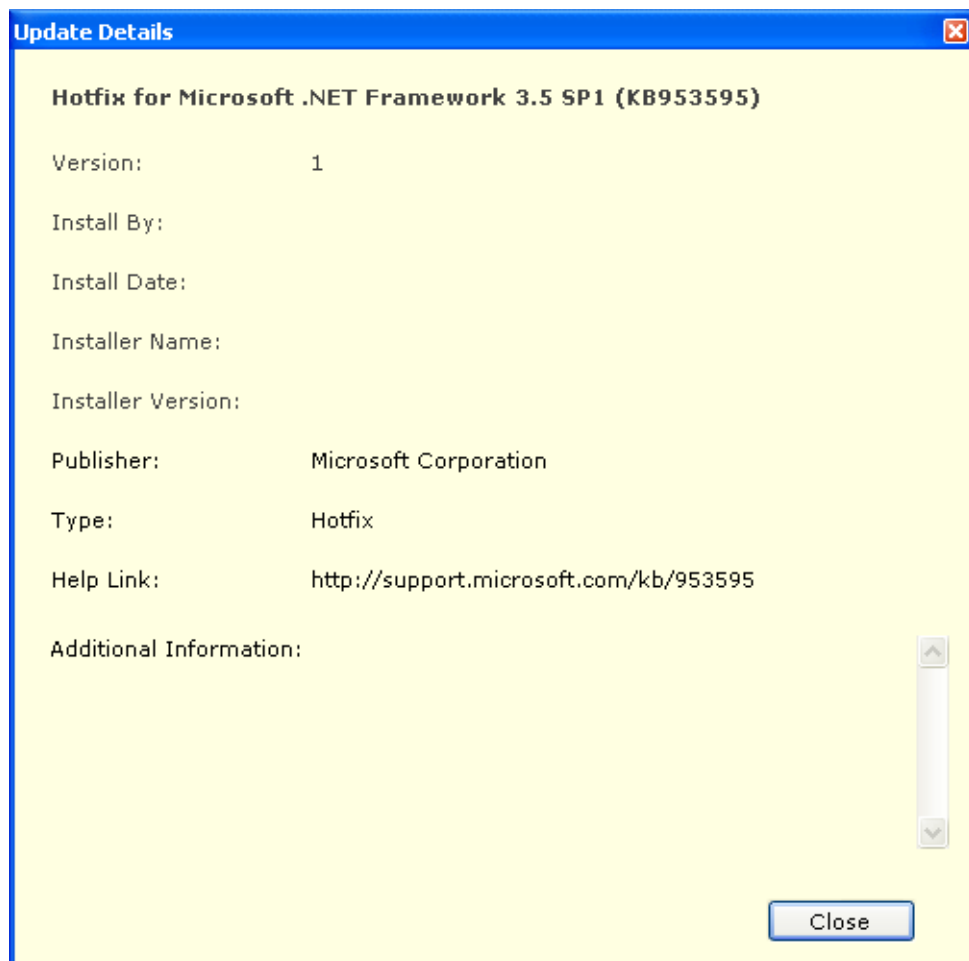
Inventory Manager displays the itemized list of hot fixes, patches, and updates installed on the selected system.

Figure 500
Updates



- 7 Click the 'here' hyperlink to view details.
Inventory Manager displays the details in a pop-up window.

Figure 501
Update details



Chapter 26

Assessing Configuration Using SCAP

In this chapter, you will learn how to:

- [Compare FDCC Policy](#)
- [View FDCC, DISA, and SCAP Scan Results](#)
- [Add Deviation](#)
- [Publish FDCC Report](#)
- [Create FDCC Report Bundle](#)

NIST Guidelines

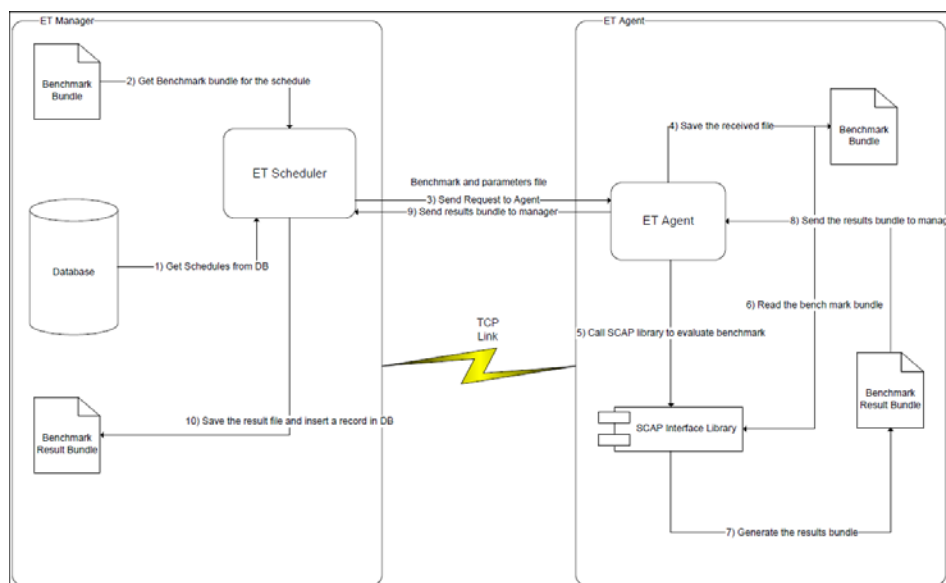
The National Institute of Standards and Technology ([NIST](#)), with sponsorship from the Department of Homeland Security ([DHS](#)), has produced Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular security level (or baseline). The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems.

How EventTracker Helps?

EventTracker Configuration Assessment module enables the agencies to automate the process of reporting compliance, with FDCC reporting requirements dictated by the standard FISMA reporting guidance.

How does it work?

Figure 502



NIST Benchmarks Implemented in EventTracker

Table 146

Benchmark Name	Description
FDCC IE 7	<p>This guide has been created to assist IT professionals in effectively securing systems with Microsoft Internet Explorer 7 installed.</p> <p>Profile: federal_desktop_core_configuration_version_1.2.0.0</p>
FDCC XP Firewall	<p>NIST Special Publication 800-68 has been created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP Professional SP2 and SP3 systems with Windows Firewall.</p> <p>Profile: federal_desktop_core_configuration_version_1.2.0.0</p>
FDCC XP Systems	<p>This benchmark has been created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP Professional SP2 systems.</p> <p>Profile: federal_desktop_core_configuration_version_1.2.0.0</p>
FDCC Vista Systems	<p>This guide has been created to assist IT professionals, in effectively securing systems with Microsoft Vista.</p> <p>Profile: federal_desktop_core_configuration_version_1.2.0.0</p>
FDCC Vista Firewall	<p>This guide has been created to assist IT professionals, in effectively securing systems with Microsoft Vista Firewall.</p> <p>Profile: federal_desktop_core_configuration_version_1.2.0.0</p>
NIST 800-68 XP Systems	<p>NIST Special Publication 800-68 has been created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP Professional SP2 systems. It discusses Windows XP and various application security settings in technical detail. The guide provides insight into the threats and security controls that are relevant for various operational environments, such as for a large enterprise or a home office. It describes the need to document, implement, and test security controls, as well as to monitor and maintain systems on an ongoing basis. It presents an overview of the security components offered by Windows XP and provides guidance on installing, backing up, and patching Windows XP systems. It discusses security policy configuration, provides an overview of the settings in the accompanying NIST security templates, and discusses how to apply additional security settings that are not included in the NIST security templates. It demonstrates securing popular office productivity applications, Web browsers, e-mail clients, personal firewalls, antivirus software, and spyware detection and removal utilities on Windows XP systems to provide protection against viruses, worms, Trojan horses, and other types of malicious code. This list is not intended to be a complete list of applications to install on Windows XP system, nor does it imply NIST endorsement of</p>

Benchmark Name	Description
	particular commercial off-the-shelf (COTS) products. Profile: federal_desktop_core_configuration_version_1.2.0.0
2003 Domain Controllers SSLF High	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Specialized-Security-Limited-Functionality-High
2003 Domain Controllers Enterprise-Low	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Enterprise-Low
2003 Domain Controllers Enterprise-Moderate	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Enterprise-Moderate
2003 Domain Controllers Enterprise-High	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Enterprise-High
2003 Domain Controllers Legacy-Low	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Legacy-Low
2003 Domain Controllers Legacy-Moderate	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Legacy-Moderate
2003 Domain Controllers Legacy-High	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-Legacy-High
2003 Domain Controllers DISA-Gold	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-DISA-Gold
2003 Domain Controllers DISA-Platinum	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Domain-Controller-DISA-Platinum
2003 Member Servers SSLF-High	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-Specialized-Security-Limited-Functionality-High
Member Servers Enterprise-Low	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-Enterprise-Low
2003 Member Servers Enterprise-	This benchmark was created based on Microsoft Windows Server 2003 Security Guide.

Benchmark Name	Description
Moderate	Profile: Member-Server-Enterprise-Moderate
2003 Member Servers Enterprise-High	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-Enterprise-High
2003 Member Servers Legacy-Low	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-Legacy-Low
2003 Member Servers Legacy-Moderate	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-Legacy-Moderate
2003 Member Servers Legacy-High	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-Legacy-High
2003 Member Servers DISA-Gold	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-DISA-Gold
2003 Member Servers DISA-Platinum	This benchmark was created based on Microsoft Windows Server 2003 Security Guide. Profile: Member-Server-DISA-Platinum
Symantec Virus Software DISA-Gold	Desktop Application Security Checklist - Symantec Virus Software has been created to assist IT professionals, in particular system administrators and information security personnel, in effectively securing Windows XP Symantec Virus Scan installations. Profile: DISA-Gold
DISA STIG XP Security	This benchmark has been created to assist IT professionals, in particular Windows XP system administrators and information security personnel, in effectively securing Windows XP Professional SP2 systems. Profile: stig
DISA STIG 2000 Security	This benchmark represents policy for the Microsoft Windows 2000 operating system. Profile: scap-win2000-profile
DISA STIG Vista Security	This guide has been created to assist IT professionals, in effectively securing systems with Microsoft Vista. Profile: stig
DISA Gold Office 2007	DISA Gold Disk - Microsoft Office System 2007. Profile: MAC_mission_critical_CONF_public_TYPE_GOLD
SCAP Office 2007	This guide has been created to assist IT professionals, in effectively securing systems with Microsoft Office 2007

Benchmark Name	Description
	installed. Profile: Specialized-Security-Limited-Functionality-rev2
USGCB IE 8	This guide has been created to assist IT professionals in effectively securing systems with Microsoft Internet Explorer 8 installed. Profile: united_states_government_configuration_baseline_version_1.0.0.0
USGCB Win7-x64	This guide has been created to assist IT professionals in effectively securing systems running Microsoft Windows 7. Profile: united_states_government_configuration_baseline_1.0.1.0
USGCB Win7-x86	This guide has been created to assist IT professionals in effectively securing systems running Microsoft Windows 7. Profile: united_states_government_configuration_baseline_1.0.1.0
USGCB Win7-x64 Firewall	This guide has been created to assist IT professionals, in effectively securing systems with Microsoft Windows 7 Firewall. Profile: united_states_government_configuration_baseline_version_1.0.0.0
USGCB Win7-x86 Firewall	This guide has been created to assist IT professionals, in effectively securing systems with Microsoft Windows 7 Firewall. Profile: united_states_government_configuration_baseline_version_1.0.0.0

What is FDCC?

FDCC stands for Federal Desktop Core Configuration. FDCC is a set of operating system configurations to help ensure security, such as turning off unused services and running user applications in user, rather than system administrator, mode. In 2007, the Office of Management and Budget (OMB) ordered that federal agencies upgrading their desktop computers, and those running Microsoft Windows XP or Windows Vista, must conform to the FDCC. FDCC is authored by the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the National Security Agency and others. For more information please refer <http://nvd.nist.gov/fdcc/index.cfm> and http://nvd.nist.gov/fdcc/fdcc_faqs_20080128.cfm.

What is SCAP?

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FDCC and FISMA compliance). The National Vulnerability Database ([NVD](#)) is the U.S. government content repository for SCAP. The Security Content Automation Protocol (SCAP), pronounced 'S-Cap', combines a number of open standards that are used to enumerate software flaws and configuration issues related to security. They measure systems to find vulnerabilities and offer methods to score those findings in order to evaluate the possible impact. It is a method for using those open standards for automated vulnerability management, measurement, and policy compliance evaluation. SCAP has two major elements. First, it is a protocol—a suite of six open specifications that standardize the format and nomenclature by which security software communicates information about software flaws and security configurations. Each specification is also known as a SCAP component. Second, SCAP includes software flaw and security configuration standardized reference data, also known as SCAP content. SCAP has several uses, including automating checks for known vulnerabilities, automating the verification of security configuration settings, and generating reports that link low-level settings to high-level requirements. SCAP defines how the following standards (referred to as SCAP 'Components') are combined:

SCAP Components

Common Vulnerabilities and Exposures (CVE) - <http://cve.mitre.org/> and [wikipedia](#)

Common Configuration Enumeration (CCE) - <http://cce.mitre.org/>

Common Platform Enumeration (CPE) - <http://cce.mitre.org/>

Common Vulnerability Scoring System (CVSS) - <http://www.first.org/cvss/> and [wikipedia](#)

Extensible Configuration Checklist Description Format (XCCDF)

Open Vulnerability and Assessment Language (OVAL)

The SCAP version allows the versions of the SCAP components to be referred to collectively.

SCAP 1.0 includes:

- XCCDF 1.1.4
- OVAL 5.3 and OVAL 5.4
- CCE 5.0
- CPE 2.2
- CVE
- CVSS 2.0

These open standards were created and are maintained by a number of different institutions including the [MITRE Corporation](#), the [NSA](#), and a special interest group

within the Forum of Incident Response and Security Teams ([FIRST](#)). NIST recommends the use of SCAP for security automation and policy compliance activities. One of the primary goals of the SCAP is to encourage the development of checklists in XML formats, particularly checklists that are compliant with XCCDF and/or OVAL.

For more information on SCAP, please refer <http://nvd.nist.gov/scap.cfm> and http://en.wikipedia.org/wiki/Security_Content_Automation_Protocol

What is SCAP content?

SCAP content or SCAP data stream consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations. The SCAP security checklist data is configuration checklists written in machine-readable languages (XCCDF). SCAP checklists have been submitted to, and accepted by, the NIST National Checklist Program. They also conform to a SCAP template and style guide to ensure compatibility with SCAP products and services. The SCAP template and style guide talks about requirements for including SCAP enumerations and mappings within the checklist. SCAP checklists refer to SCAP test procedures (low level checks of machine state written in OVAL). SCAP test procedures are used in conjunction with SCAP checklists (<http://nvd.nist.gov/ncp.cfm?scap>).

SCAP content is a collection of four or more related XML files containing SCAP data using the SCAP components that provide the data necessary to evaluate systems for compliance with a configuration-based security policy. Patch checking content may also be included in this bundle. Files included for SCAP 1.0 are listed below, with the 'XXXX' in each name representing a unique prefix for the bundle (e.g., fdcc-xp, fdcc-vista):

- XXXX-xccdf.xml - XCCDF 1.1.4 content
 - XXXX-cpe-oval.xml - CPE OVAL 5.3 definitions
 - XXXX-cpe-dictionary.xml - Minimal CPE 2.2 dictionary
 - XXXX-oval.xml - OVAL 5.3 compliance definitions
-

How SCAP is Implemented in EventTracker

EventTracker supports the following SCAP capabilities:

- Federal Desktop Core Configuration (FDCC) Scanner
- Authenticated Configuration Scanner
- Authenticated Vulnerability and Patch Scanner

EventTracker implements the SCAP 1.0 standard by implementing

- Common Vulnerability Enumeration (CVE)
- Common Configuration Enumeration (CCE)

- Common Platform Enumeration (CPE)
- Extensible Configuration Checklist Documentation Format (XCCDF)
- Open Vulnerability Assessment Language (OVAL) [EventTracker uses MITRE's reference implementation of OVAL]

EventTracker contains in-built SCAP content for FDCC and other benchmarks. EventTracker also allows the user to validate and import the latest SCAP content for the in-built benchmarks. EventTracker provides a Web interface that can be used to schedule the assessment or perform on demand assessment against the systems that have EventTracker agent installed on them. EventTracker user interface contains references to CCE entries for each of the rule results. Where applicable, the results also contain OVAL reference, CVE references, and CPE references. Each target system is assessed using CPE dictionary and has its operating system identified with a CPE reference. All CVE references have an external link to NVD.

What is CVE?

CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Source: <http://cve.mitre.org/>

How CVE Standard is Implemented in EventTracker

Prism Microsystems EventTracker implements the CVE standard by displaying appropriate CVE identifiers with every definition result for which such an identifier exists; these are predominantly definition results that have a Definition Class of "vulnerability" or "patch". These CVE identifiers are extracted from the SCAP content imported by EventTracker.

EventTracker user interface contains link to an HTML report of results of patch content that is part of the imported SCAP content. For every definition result for which a CVE identifier is available, the CVE identifier is displayed within this HTML report. Each CVE identifier is expressed as a link to the NVD site. These links are displayed irrespective of whether or not the vulnerability is actually present, as they are associated with definition results within the imported SCAP content.

What is CCE?

CCE™ provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools.

Source: <http://cce.mitre.org/>

How CCE Standard is Implemented in EventTracker

Prism Microsystems EventTracker implements the CCE standard by displaying appropriate CCE identifiers with every definition result for which such an identifier exists; these are predominantly definition results that have a Definition Class of "compliance". These CCE identifiers are extracted from the SCAP content imported by EventTracker.

In addition to displaying the CCE identifiers in user interface that displays XCCDF rule results, EventTracker allows the user to export the assessment results in MS Excel format. EventTracker allows the user to export the assessment results in the comma separated format that contains CCE identifier and the rule result. EventTracker also includes a search feature that allows users to search the assessment results for a given CCE identifier.

What is CPE?

CPE™ is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

Source: <http://cpe.mitre.org/>

How CPE Standard is Implemented in EventTracker

Prism Microsystems EventTracker implements the CPE 2.2 standard by displaying appropriate CPE identifiers with every definition result for which such an identifier exists; these are predominantly definition results that have a Definition Class of "inventory". These CPE identifiers are extracted from the SCAP content imported by EventTracker. EventTracker checks for validity of a benchmark against the target system using the CPE dictionary and CPE OVAL definitions that are included in the SCAP content. Each target system is assessed using CPE dictionary and has its operating system identified with a CPE reference. EventTracker user interface contains link to an HTML report of results of CPE definitions that is part of the imported SCAP content. For every definition result for which a CPE identifier is available, the CPE identifier is displayed within this HTML report.

What is XCCDF?

XCCDF stands for Extensible Configuration Checklist Description Format and it is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. Checklists can be developed using many different formats; however, having standard formats supports

interoperability and ease of use. XCCDF can define structured collections of security configuration rules for sets of target systems. The XCCDF specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices. For more information refer <http://nvd.nist.gov/xccdf.cfm> and <http://en.wikipedia.org/wiki/XCCDF>.

How XCCDF Standard is Implemented in EventTracker

Prism Microsystems EventTracker implements the XCCDF 1.1.4 standard by providing the capability of directly importing SCAP content. The SCAP content itself is composed of a bundle of XML files, some of which are in XCCDF-compliant format. EventTracker contains a validation routine that checks XCCDF files against schema documents, and reports any errors during the import process.

Before processing the XCCDF content of the benchmark, if required EventTracker resolves the XCCDF file as per the specification. After resolving the XCCDF file, EventTracker applies the profile specified in the input and, if required, generates OVAL external variables file. Along with displaying the assessment results in the user interface, EventTracker generates XCCDF results file according to the specification and schema documents. The user interface also allows a user to declare deviations, create Plans of Actions and Milestones (POA&Ms) for the associated remediation and use the output XCCDF for configuration reporting to authoritative oversight organizations.

What is OVAL?

Another language widely used for checklists. 'Open Vulnerability and Assessment Language' (OVAL) is utilized by security experts to exchange technical details about how to check for the presence of vulnerabilities and configuration issues on computer systems. The vulnerabilities and configuration issues are identified using tests—OVAL definitions in Extensible Markup Language (XML)—that can be utilized by end users or implemented in information security products and services. OVAL provides a standard XML format for vulnerability identification and scan criteria for vulnerabilities. More information on OVAL is available at <http://oval.mitre.org/>. A set of instructions used to check for a security problem, such as an incorrect minimum password length setting, is known as an OVAL definition. A file containing one or more OVAL definitions (often hundreds or even thousands) is known as an OVAL definition file. A single definition file often contains many more tests than would ever be run against a single system; for example, a file could contain checks for minimum password lengths of at least 8 characters and at least 12 characters, but typically at most one of these two checks would be run against a particular system. Actually, the intention of the SCAP is not to have OVAL definition files used

directly to perform checks on systems, but rather to have an XCCDF file use just the OVAL definitions that are needed to check a particular system.

How OVAL Standard is Implemented in EventTracker

Prism Microsystems EventTracker implements the OVAL standard by providing the capability of directly importing SCAP content. The SCAP content itself is composed of a bundle of XML files, some of which are in OVAL format. EventTracker contains a validation routine that checks OVAL files against OVAL definition schematron, and reports any errors during the import process. EventTracker uses MITRE's reference implementation of OVAL as the SCAP checking engine.

What is CVSS?

CVSS is an open framework that helps organizations prioritize vulnerabilities so that they can remediate higher priority vulnerabilities sooner than lower priority vulnerabilities.

How EventTracker supports CVSS

EventTracker fully supports version 2.0 of the Common Vulnerability Scoring System (CVSS) standard to the extent that is required for providing a SCAP validated tool with FDCC Scanner capability.

Each Common Vulnerabilities and Exposures (CVE) entry has a CVSS vector for calculating the relative severity of vulnerabilities. Currently, the SCAP XCCDF input data streams for FDCC available on the National Vulnerabilities Database (NVD) Web site assign the same priority to all compliance checks and these priorities are compatible with CVSS.

EventTracker preserves the only CVE relationships that exist in the FDCC data stream embodied in the references established by the PatchesUpToDate rule. These references, which are to the actual OVAL definitions, will resolve to the fdcc-xxxx-patches document or the information published on the NVD web site, depending on Internet connectivity. The CVE references to the NVD web site provide access to CVSS information including CVSS vectors and CVSS base scores. The NVD website also provides an overview of the vulnerability, affected platforms and references to other external sources like – Vendor specific security alerts/bulletins, US-CERT, Bugtraq, Open Source Vulnerability Database (OSVDB) etc.

EventTracker does not use CVSS or display CVSS data.

FDCC and SCAP

While FDCC represents a specific security and configuration standard to which systems must adhere, The Security Content Automation Protocol (SCAP) is a far

broader initiative to ensure a level of standardization and interoperability within the security community for vulnerabilities and system configuration definitions.

It is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). While the specific standards that comprise SCAP are beyond the scope of this short paper, it is worth noting that any tool used to automate FDCC assessments and management must itself be SCAP validated.

FDCC Reporting Format

There are two distinct portions of FDCC compliance reporting. The first portion involves submitting an SCAP XCCDF document for each environment present within an organization. The second portion involves submitting an Excel workbook that provides a high level summary of every environment present within the organization. This Excel workbook aggregates the data collected in the SCAP XCCDF report documents. Each environment listed within the Excel workbook must reference the corresponding SCAP XCCDF document. In a FDCC report an agency should report Computer counts, SCAP XCCDF reports, and FDCC deviations for each operational environment/system role present within the Agency. The possible operational environments are:

- Centrally Managed General Purpose Desktop: The desktop systems run end-user productivity applications (e.g., email clients, word processors). The desktop systems are joined to a native Windows active directory environment where the policy is managed through GPOs.
- Centrally Managed General Purpose Laptop: The laptop systems run end-user productivity applications (e.g., email clients, word processors). The laptop systems are joined to a native Windows active directory environment where the policy is managed through GPOs.
- Development System: The systems are used to perform development-related tasks.
- Special Use System: The systems perform a special task that does not fit into any of the above categories (e.g., laboratory/research systems, kiosk systems, SCADA systems).
- Other: The systems cannot be grouped into any of the above categories. This includes desktops and laptops that are not centrally managed. If this choice is selected, a detailed description must be provided in the "Environment Description" column of the spreadsheet.

Please refer http://nvd.nist.gov/fdcc/fdcc_reporting.cfm and http://nvd.nist.gov/fdcc/fdcc_faqs_20080128.cfm for detailed information about the FDCC reporting requirements and format.

Assessing Managed Computers

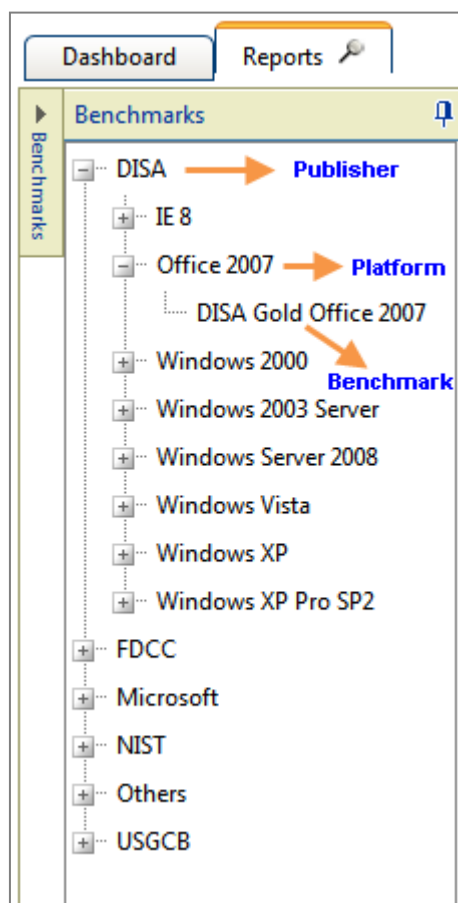
You can scan a computer for compliance benchmarks in the same manner as it is done to compare Change Policies.

Grouping of benchmarks with respect to Publisher and Platform

Move the mouse pointer over **Config Assessment**, and then select **Reports** from the dropdown list.

On the left hand side, you can see the benchmarks are grouped under publisher and platform.

Figure 503



Viewing Assessment Results

This option helps you view assessment results on the Config Assessment Dashboard.

To view assessment results

- 1 Log on to EventTracker Enterprise.
- 2 Click **Config Assessment**.
- 3 Click the **Reports** tab.

EventTracker displays the Reports tab.

Figure 504
Configuration
Assessment -
Success

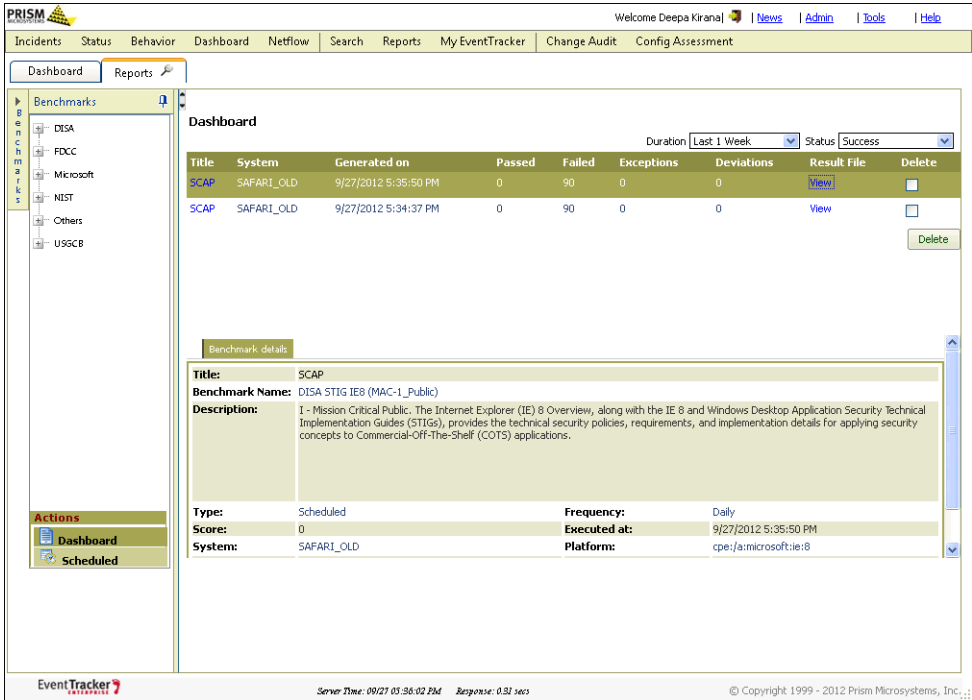


Table 147

Field	Description
Top Pane	
Title	Title of the Configuration Assessment schedule.
System	Name of the system against which the benchmarks were compared.
Passed	Benchmark rules that found to comply.
Failed	Benchmark rules that failed to comply.
Exceptions	A rule with the result "error", "unknown", "not applicable", "not checked", "not selected", "informational", or "fixed" is considered as an exception.
Deviations	Rules that are not implemented on the managed systems could be declared as deviations with reasons why and when it could be implemented.
Result File	Click the View hyperlink to view the result file.
Duration	Select an option to view benchmark comparison execution by period. Duration ranges from 1 day to 12 months.
Status	Select an option to view configuration assessment result by status. Valid options are Success and Fail .
Bottom Pane displays the Benchmark details.	

Figure 505
Configuration
Assessment - Fail

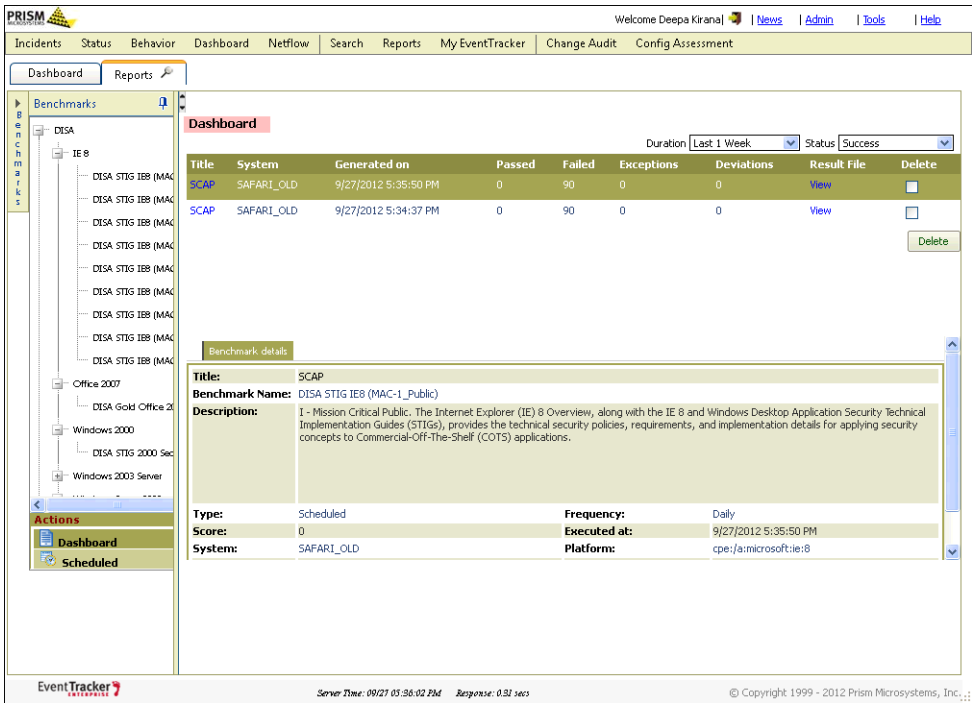


Table 148

Field	Description
Top Pane	
Title	Title of the policy comparison.
System	Name of the system against which the benchmarks were compared.
Generated on	Date and time when the benchmark comparison was executed.
Reason	Reason for why the benchmark comparison failed to execute.
Bottom Pane displays the Benchmark details.	

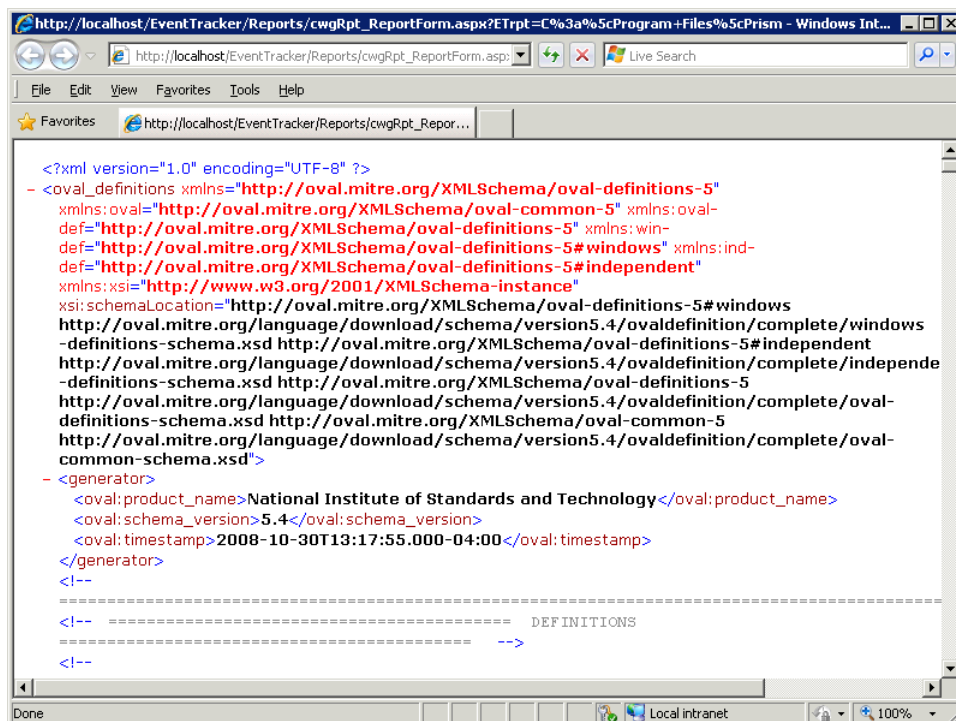
Note



EventTracker displays hyperlinks in the Title column only for the successful configuration assessment.

- 4 Select **Success** or **Fail** from the **Status** drop-down list.
- 5 Scroll down the Benchmark details pane and click **View Oval definitions XML** hyperlink.
EventTracker displays the File Download pop-up window.
- 6 Click **Open** to view OVAL definitions.

Figure 506
OVAL definitions



Viewing Assessment Details

This option helps you view assessment details.

To view assessment details

- 1 Click a title of the schedule in the top pane.
EventTracker displays the Config Assessment results page.

Figure 507
Config Assessment
results

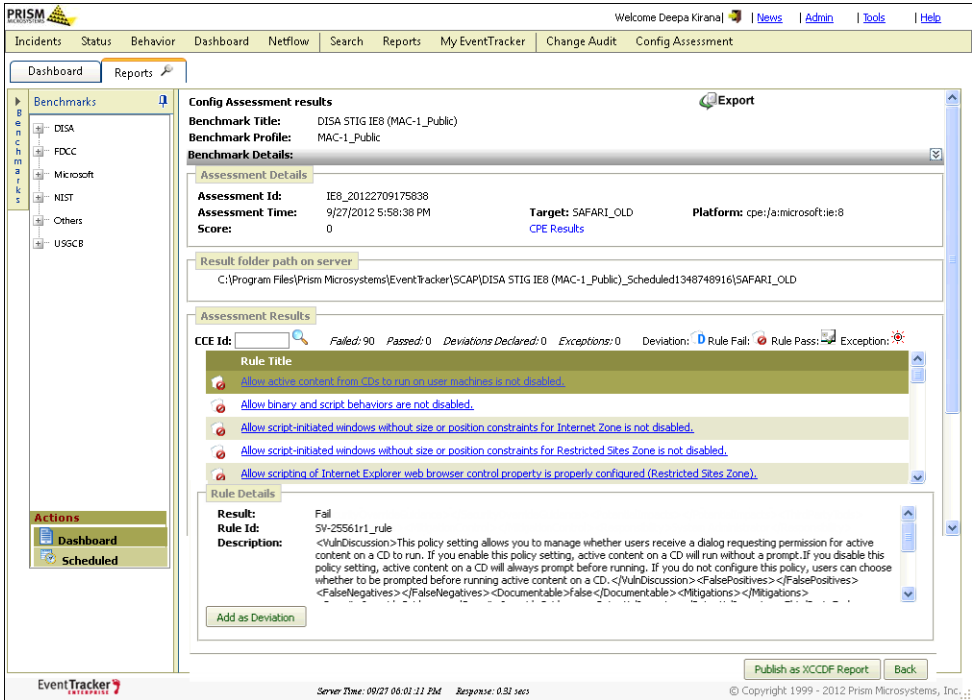


Table 149

Icon	Represents
	A failed rule marked as Deviation. You can declare failed rule as deviation with proper rationale and tentative time frame when it could be rectified.
	Rule that failed to comply.
	Rule that complied.
	A rule with the result "error", "unknown", "not applicable", "not checked", "not selected", "informational", or "fixed" is considered an exception.

- Click the button to view description of the Benchmark.
- Click a Rule in the Assessment Results pane to view Rule details.
- Click the **CPE Results** hyperlink.

EventTracker displays CPEOVAL results.

Figure 508
CPEOVAL results

The screenshot shows the 'OVAL Results' page in a Windows Internet Explorer browser. The address bar shows a local host URL. The page content is organized into several sections:

- OVAL Results Generator Information:** A table with columns for Schema Version, Product Name, Product Version, Date, and Time. It shows version 5.6 for 'OVAL Definition Interpreter'.
- OVAL Definition Generator Information:** A table with columns for Schema Version, Product Name, Product Version, Date, and Time. It shows version 5.4 for 'National Institute of Standards and Technology'.
- System Information:** A table listing system details:

Host Name	webdoc1.Toons.local						
Operating System	Microsoft Windows XP Professional Service Pack 3						
Operating System Version	5.1.2600						
Architecture	INTEL32						
Interfaces	<table border="1"> <tr><td>Interface Name</td><td>Realtek RTL8139 Family PCI Fast Ethernet NIC - Teefer2 Miniport</td></tr> <tr><td>IP Address</td><td>192.168.1.88</td></tr> <tr><td>MAC Address</td><td>00-14-85-49-B6-C9</td></tr> </table>	Interface Name	Realtek RTL8139 Family PCI Fast Ethernet NIC - Teefer2 Miniport	IP Address	192.168.1.88	MAC Address	00-14-85-49-B6-C9
Interface Name	Realtek RTL8139 Family PCI Fast Ethernet NIC - Teefer2 Miniport						
IP Address	192.168.1.88						
MAC Address	00-14-85-49-B6-C9						
- OVAL System Characteristics Generator Information:** A table with columns for Schema Version, Product Name, Product Version, Date, and Time. It shows version 5.6 for 'OVAL Definition Interpreter'.
- OVAL Definition Results:** A table with columns for ID, Result, Class, Reference ID, and Title. It includes a legend for True (orange), False (green), Error (yellow), Unknown (blue), Not Applicable (grey), and Not Evaluated (white).

ID	Result	Class	Reference ID	Title
oval.org.mitre.oval.def.5631	true	inventory	cpe:/o:microsoft:windows_xp::sp3:x86	Microsoft Windows XP SP3 is installed
oval.org.mitre.oval.def.754	false	inventory	cpe:/o:microsoft:windows_xp::sp2:x86	Microsoft Windows XP SP2 is installed

- Click the **Patch Results** hyperlink.
EventTracker displays PatchOVAL results.

Figure 509

OVAL Results Generator Information					OVAL Definition Generator Information				
Schema Version	Product Name	Product Version	Date	Time	Schema Version	Product Name	Product Version	Date	Time
5.6	OVAL Definition Interpreter	5.6 Build: 3	2010-11-02	15:45:51	5.3	National Institute of Standards and Technology		2010-06-15	19:30:33

System Information	
Host Name	webdoc1.Toons.local
Operating System	Microsoft Windows XP Professional Service Pack 3
Operating System Version	5.1.2600
Architecture	INTEL32
Interfaces	Interface Name: Realtek RTL8139 Family PCI Fast Ethernet NIC - Teefer2 Miniport
	IP Address: 192.168.1.88
	MAC Address: 00-14-85-49-B6-C9

OVAL System Characteristics Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.6	OVAL Definition Interpreter	5.6 Build: 3	2010-11-02	15:45:39

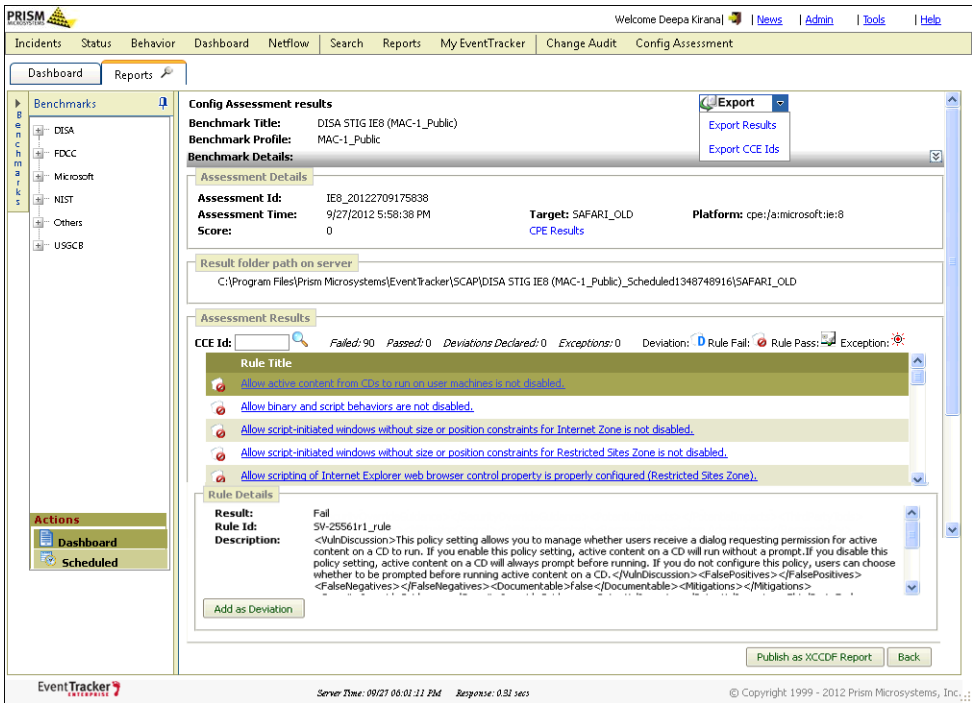
Exporting Assessment Details

This option helps you export assessment details.

To export assessment details

- 1 Click **Export**.

Figure 510
Export



- From the drop-down list, choose **Export Results** to export Configuration Assessment results into Excel format.
- From the drop-down list, choose **Export CCE Ids** to export summary report on Passed, Failed, and Exception CCE Ids into Excel format.

Searching Rules by CCE Id

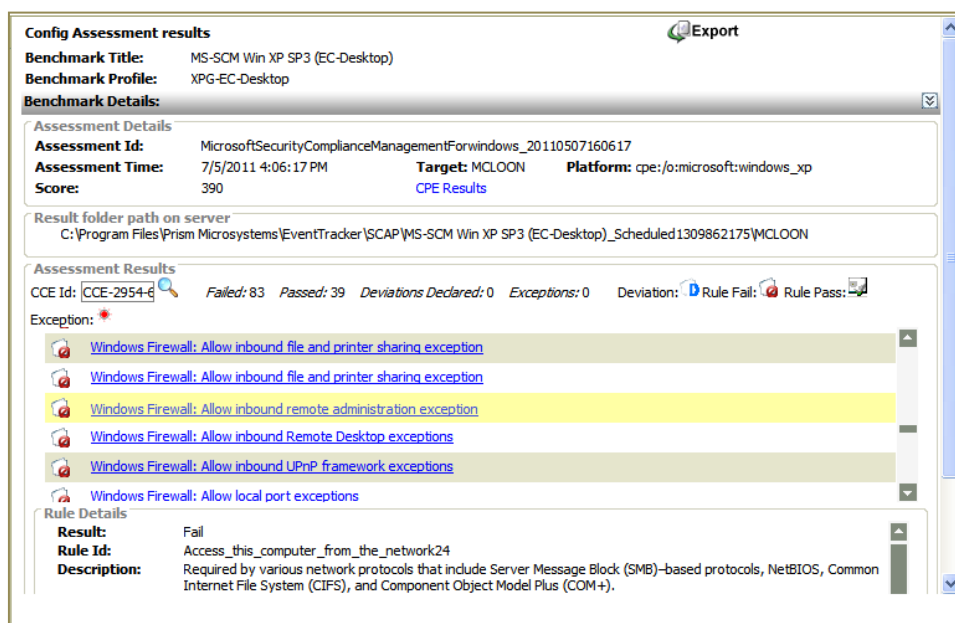
This option helps you search benchmark rules by CCE Id.

To search rules by CCE Id

- To search rules by CCE Id, type the CCE Id in the **CCE Id** field and then click .
Ex: CCE-2954-6.

EventTracker displays the message box with count of matches found and highlights search result in yellow color.

Figure 511
CCE Id search



Adding Deviation

To add a rule as deviation

- 1 Click a failed rule.
- 2 Click **Add as Deviation**.

EventTracker displays the Deviation Details window.

Figure 512
Deviation Details

The screenshot shows a window titled "Deviation Details" with a standard Windows-style title bar (minimize, maximize, close buttons). Inside the window, there are several input fields and checkboxes:

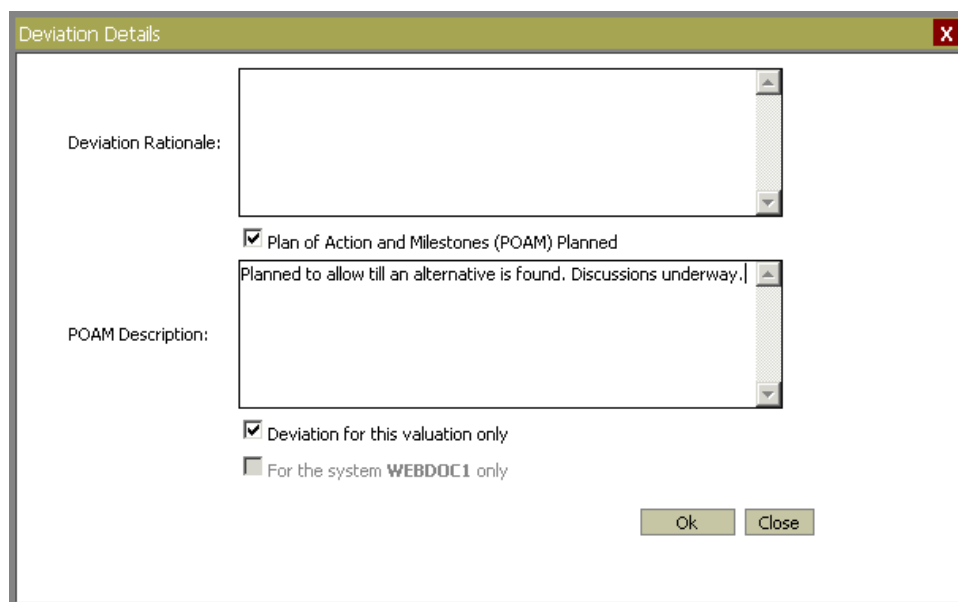
- Deviation Rationale:** A large text area for entering the reason for the deviation.
- Plan of Action and Milestones (POAM) Planned:** A checkbox to indicate if a POAM is planned.
- POAM Description:** A text area for describing the planned action.
- Deviation for this valuation only:** A checkbox to limit the deviation to the current valuation.
- For the system WEBDOC1 only:** A checkbox to limit the deviation to the specific system "WEBDOC1".
- Buttons:** "Ok" and "Close" buttons are located at the bottom right of the dialog.

Table 150

Field	Description
Deviation Rationale	Type a valid reason why this rule was breached.
Plan of Action and Milestones [POAM] planned	Select this checkbox. EventTracker enables the POAM Description field.
POAM Description	Type the course action that would be taken to rectify the deviation.
Deviation for this evaluation only	Select this checkbox if you wish EventTracker to remember the deviation for this evaluation only. Otherwise, EventTracker will remember for all evaluations. EventTracker hides the 'Mark the deviation for this system only' checkbox.
Mark the deviation for (System Name) system only	Select this checkbox if you wish EventTracker to remember the deviation for this system only. Otherwise, EventTracker will remember for all systems.

3 Enter/select appropriately and then click **OK**.

Figure 513
Deviation Details

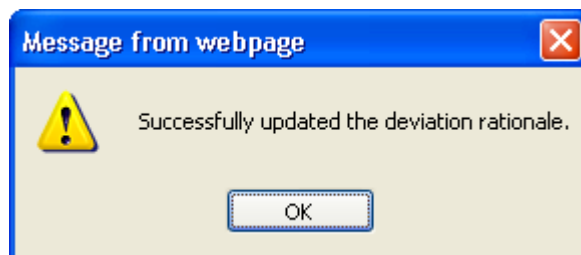


The 'Deviation Details' dialog box contains the following elements:

- Deviation Rationale:** A large text area for entering the rationale.
- POAM Description:** A text area containing the text: "Planned to allow till an alternative is found. Discussions underway."
- Plan of Action and Milestones (POAM) Planned:** A checked checkbox.
- Deviation for this valuation only:** A checked checkbox.
- For the system WEBDOC1 only:** An unchecked checkbox.
- Buttons:** 'Ok' and 'Close' buttons at the bottom right.

EventTracker displays the message box after successfully updating the deviation rationale.

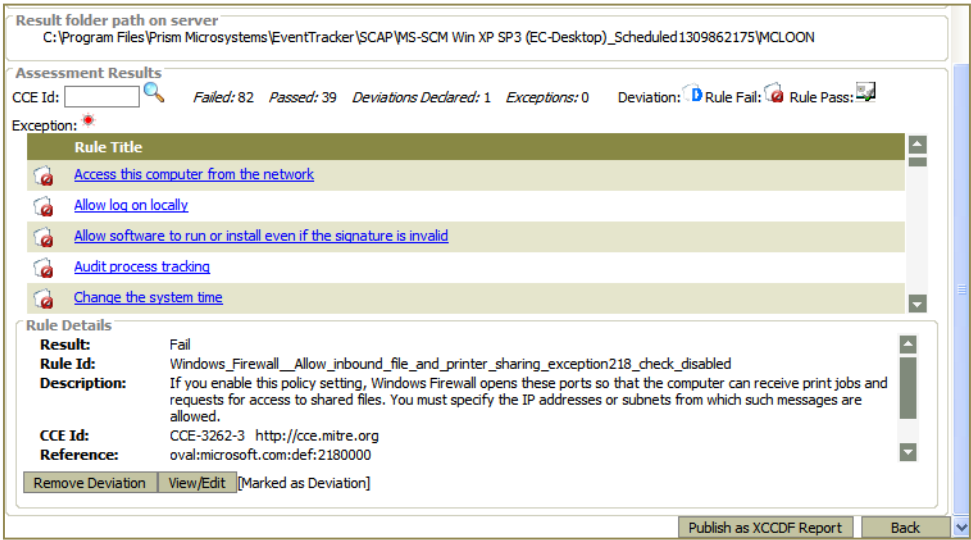
Figure 514



- 4 Click **OK**.

EventTracker displays the **Remove Deviation** and **View/Edit** buttons on the FDCC Compliance Results window.

Figure 515
Deviation Details



Publishing FDCC Report

To publish FDCC report

- 1 Click **Publish as XCCDF Report**.

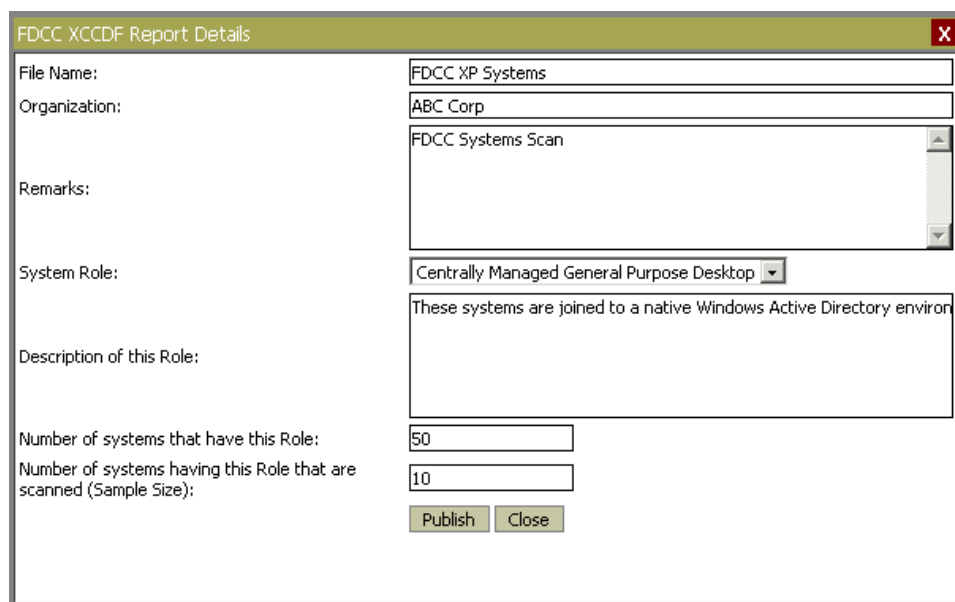
EventTracker displays the FDCC XCCDF Report Details window.

Figure 516
FDCC XCCDF Report
Details

The screenshot shows the 'FDCC XCCDF Report Details' window. It contains several input fields: 'File Name:', 'Organization:', 'Remarks:', 'System Role:' (with a dropdown menu showing 'Centrally Managed General Purpose Desktop'), 'Description of this Role:', 'Number of systems that have this Role:', and 'Number of systems having this Role that are scanned (Sample Size)'. At the bottom, there are 'Publish' and 'Close' buttons.

- 2 Enter/select appropriately in the relevant fields.

Figure 517
FDCC XCCDF Report
Details



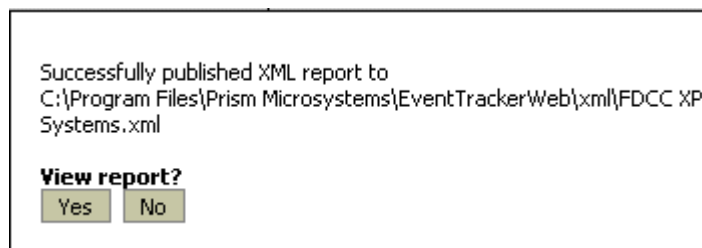
The dialog box titled "FDCC XCCDF Report Details" contains the following fields and controls:

- File Name:** Text box containing "FDCC XP Systems".
- Organization:** Text box containing "ABC Corp".
- Remarks:** Text area containing "FDCC Systems Scan".
- System Role:** Dropdown menu showing "Centrally Managed General Purpose Desktop".
- Description of this Role:** Text area containing "These systems are joined to a native Windows Active Directory environ".
- Number of systems that have this Role:** Text box containing "50".
- Number of systems having this Role that are scanned (Sample Size):** Text box containing "10".
- Buttons:** "Publish" and "Close" buttons at the bottom right.

- 3 Click **Publish**.

EventTracker displays the message box after successfully publishing the report.

Figure 518
Published
successfully –
message box



The message box contains the following text and controls:

- Text: "Successfully published XML report to C:\Program Files\Prism Microsystems\EventTracker\Web\xml\FDCC XP Systems.xml"
- View report?** label above two buttons: "Yes" and "No".

- 4 Click **Yes** to view report.

(OR)

Click **No** to close the window.

Viewing OVAL Result File

This option helps to view OVAL result file.

To view OVAL result file

- 1 Click **Dashboard** on the Actions pane.
- 2 On the top pane, click the **View** hyperlink in the **Result File** column.
EventTracker displays the File Download pop-up window.
- 3 Click **Save** to save the result file in a safer location for future reference.

- 4 Click **Open** to view the contents of the file.
EventTracker displays the OVAL results.

Figure 519
OVAL results

The screenshot shows a web browser window titled "OVAL Results - Windows Internet Explorer". The address bar shows a URL starting with "http://localhost/EventTracker/Reports/cwgRpt_ReportForm.aspx?". The page content is divided into several sections:

- OVAL Results Generator Information**: A table with columns Schema Version, Product Name, Product Version, Date, and Time. It shows Schema Version 5.6, Product Name OVAL Definition Interpreter, Product Version 5.6 Build: 3, Date 2010-12-03, and Time 10:45:42.
- OVAL Definition Generator Information**: A table with columns Schema Version, Product Name, Product Version, Date, and Time. It shows Schema Version 5.4, Product Name National Institute of Standards and Technology, Product Version, Date 2008-10-30, and Time 13:17:55.
- System Information**: A table with rows for Host Name (webdoc1.Toons.local), Operating System (Microsoft Windows XP Professional Service Pack 3), Operating System Version (5.1.2600), Architecture (INTEL32), and Interfaces (Interface Name: Realtek RTL8139 Family PCI Fast Ethernet NIC - Teefer2 Miniport, IP Address: 192.168.1.88, MAC Address: 00-14-85-49-B6-C9).
- OVAL System Characteristics Generator Information**: A table with columns Schema Version, Product Name, Product Version, Date, and Time. It shows Schema Version 5.6, Product Name OVAL Definition Interpreter, Product Version 5.6 Build: 3, Date 2010-12-03, and Time 10:45:42.
- OVAL Definition Results**: A table with columns ID, Result, Class, Reference ID, and Title. It lists several OVAL definitions and their results, including "Microsoft Windows XP SP3 is installed", "Define port exceptions - Domain Profile", "Allow remote administration exceptions disable - Standard Profile", "Allow file and print sharing exception - Domain Profile", "Microsoft Windows XP SP2 is installed", and "Allow ICMP exceptions (Allow inbound echo request and block everything else) - Domain Profile".

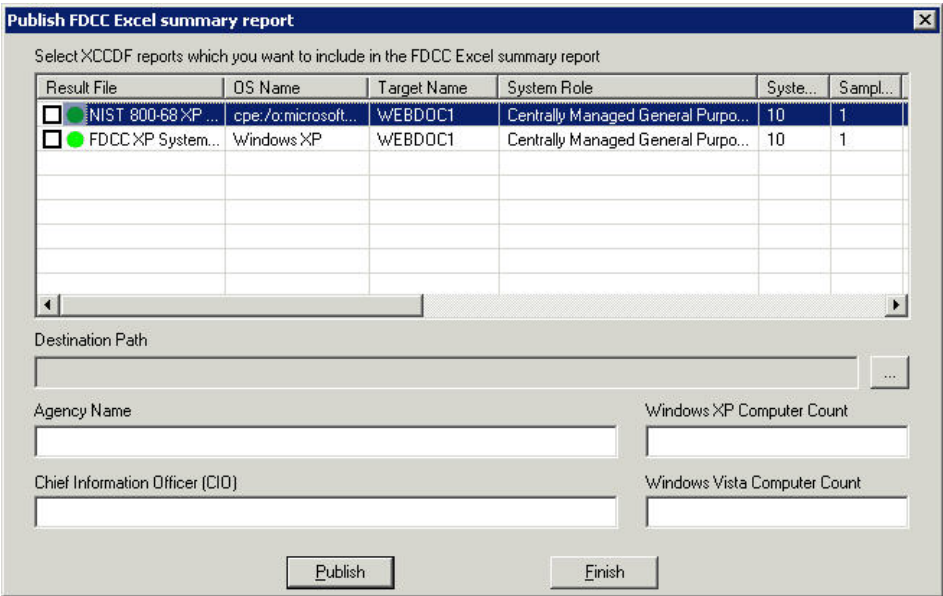
Creating FDCC Report Bundle

This option helps to create an Excel summary report with the XML file(s) created earlier.

To create FDCC report bundle

- 1 Double-click **Change Audit** on the EventTracker Control Panel.
EventTracker displays the Results Summary Console.
- 2 Click the **Tools** menu and select the **Create FDCC Report Bundle** option.
EventTracker displays the 'Publish FDCC Excel summary' report window.

Figure 520
Publish FDCC Excel
summary report



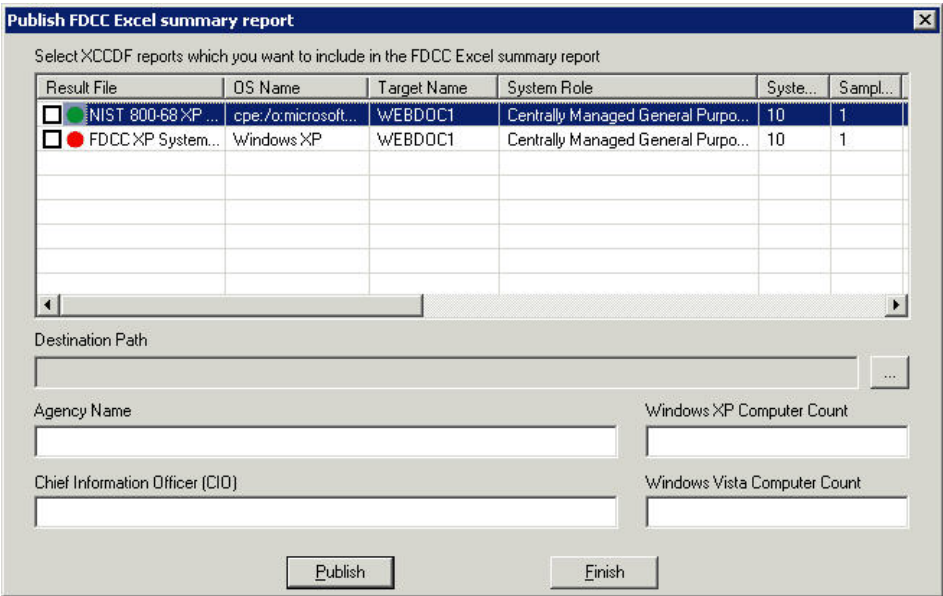
Note



EventTracker lists only the latest XML file(s).

EventTracker displays a red icon if the XML file does not exist physically.

Figure 521
Publish FDCC Excel
summary report

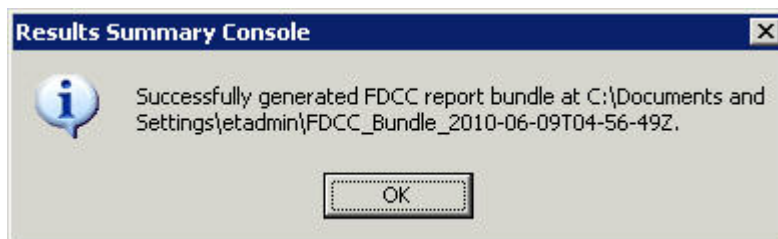


- 3 Select the XML file(s).
- 4 Click the browse button and select the destination folder.

- 5 Type appropriately in the relevant fields.
- 6 Click **Publish**.

After successfully creating the report bundle, EventTracker displays the success message box.

Figure 522
Published
successfully –
message box



- 7 Click **OK**.
- 8 Click **Finish**.

If there is no XCCDF report is published for FDCC bundle, EventTracker displays the informative message box to publish XCCDF report.

Figure 523
Informative
message box



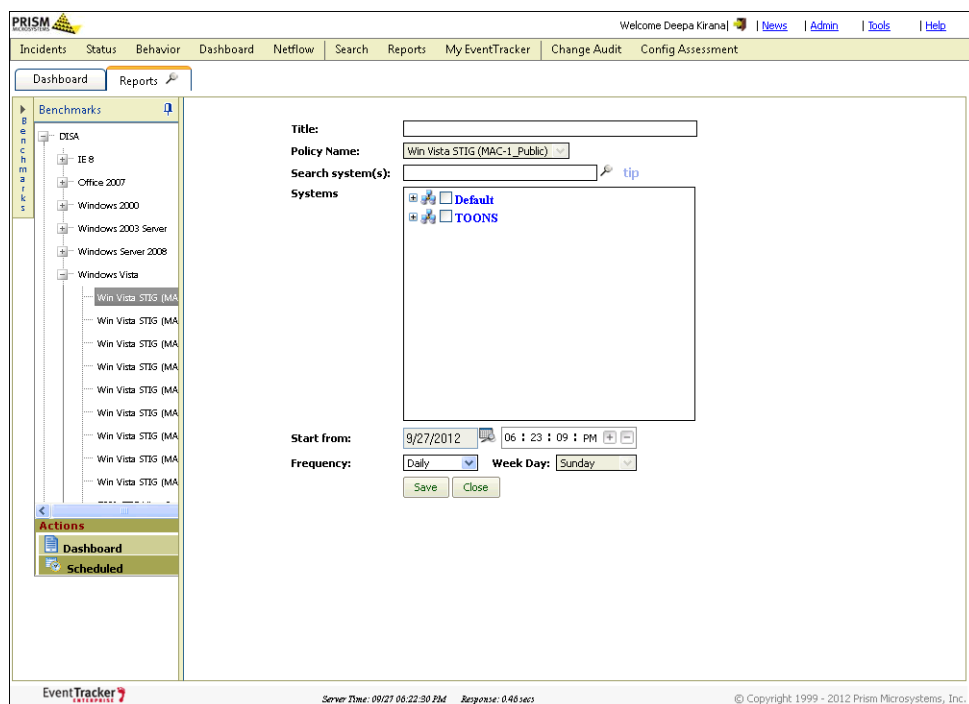
Scheduling Config Assessment

This option helps to schedule Config Assessment.

To schedule Config Assessment

- 1 Logon to **EventTracker Enterprise**.
- 2 Click **Config Assessment**.
- 3 Click **Reports** tab.
- 4 Click **Scheduled** on the 'Actions' pane.
EventTracker displays the Scheduled page.
- 5 Click **New Schedule** button on the bottom pane.

Figure 524
New schedule



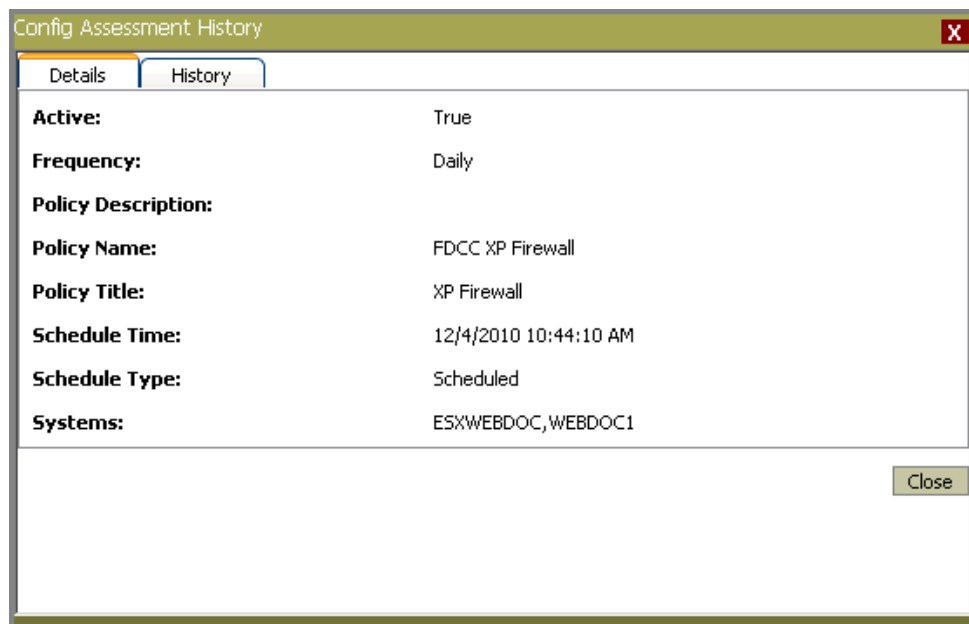
- 6 Type the title of the schedule in the **Title** field.
- 7 Select a policy from the **Policy Name** drop-down list.
- 8 Move the mouse pointer over **Tip** to view search hints.
- 9 Type the name of the system(s) in the **Search system(s)** field and then click the search icon.
EventTracker displays the system group of the systems searched.
- 10 Select the system(s).
- 11 Click **Show All** to view all managed systems and system groups.
(OR)
Select system(s)/system group(s) from the **Systems** list.
- 12 Set date and time, when to run the schedule.
- 13 Select an option from the **Frequency** drop-down list for how often the policy should be run.
EventTracker enables the **Week Day** drop-down list only when you select the **Weekly** option from the **Frequency** drop-down list.
- 14 Click **Save**.

Viewing Schedule Details and History

To view schedule details and history

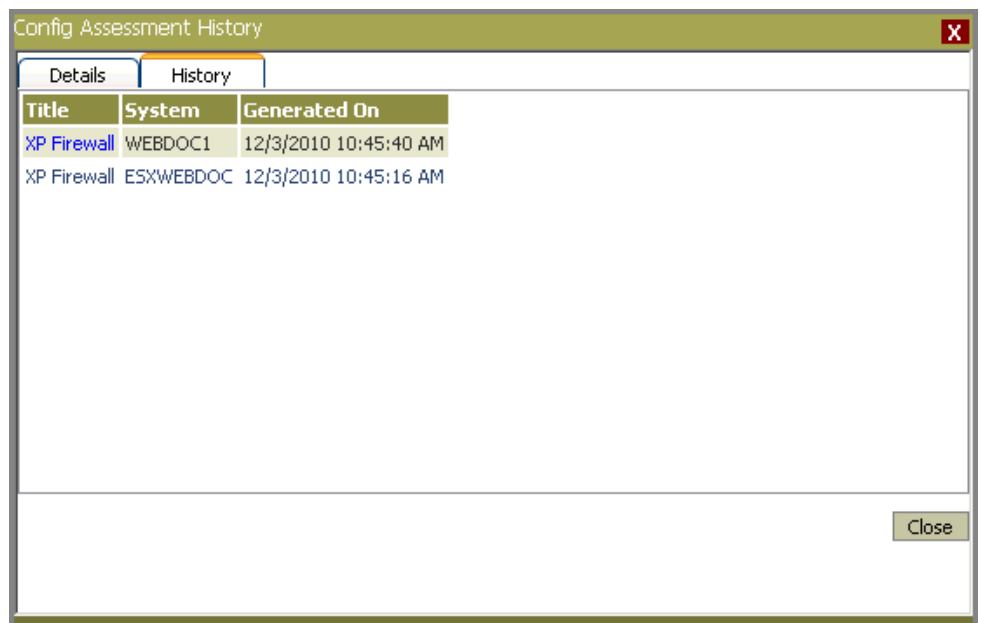
- 1 On the bottom pane, click the hyperlink in the **Title** column.
EventTracker displays the Config Assessment History window.

Figure 525
Details



- 2 Click the **History** tab to view schedule execution history.

Figure 526
History



The screenshot shows a window titled 'Config Assessment History' with a close button (X) in the top right corner. The window has two tabs: 'Details' and 'History'. The 'History' tab is selected, displaying a table with three columns: 'Title', 'System', and 'Generated On'. The table contains two rows of data.

Title	System	Generated On
XP Firewall	WEBDOC1	12/3/2010 10:45:40 AM
XP Firewall	ESXWEBDOC	12/3/2010 10:45:16 AM

A 'Close' button is located in the bottom right corner of the window.

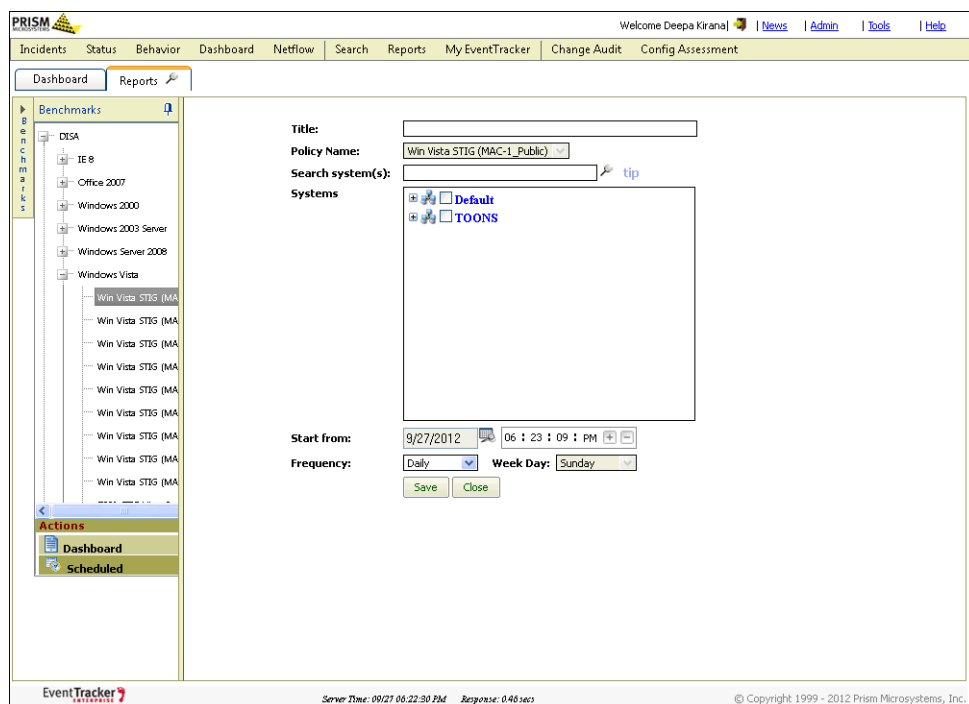
Editing Config Assessment Schedules

This option helps to edit Config Assessment schedules.

To edit Config Assessment schedules

- 1 Select a schedule on the bottom pane.
- 2 Click **Edit**.

Figure 527
Editing schedules



- 3 Make changes appropriately in the relevant fields.
- 4 Click **Save**.

Searching Published Reports

This option helps to search generated scheduled reports.

To search published reports


- 1 Select a schedule on the bottom pane.
 - 2 Click the search button .
- EventTracker displays the Published report search window.


Figure 528
Published report
search

- 3 Type the name of the report in the **Title** field.
- 4 Select date and time in **From** and **To** field.
- 5 Click **Search**.
- 6 Click **Reset** to clear all fields and start search afresh.

Exporting Summary on Published Reports

This option helps to export summary report on published reports in Excel format.

To export Summary report

- 1 Click the Export button .
EventTracker displays the File Download pop-up window.
- 2 Click **Save** to save the file in a safer location for future reference.
- 3 Click **Open** to view the contents of the file.

Importing SCAP Benchmarks

This option helps you update FDCC Benchmark rules supplied with EventTracker. SCAP Content Import Utility validates the Benchmark rules before importing. If the rules fail to validate, the existing rules are retained intact.

Note



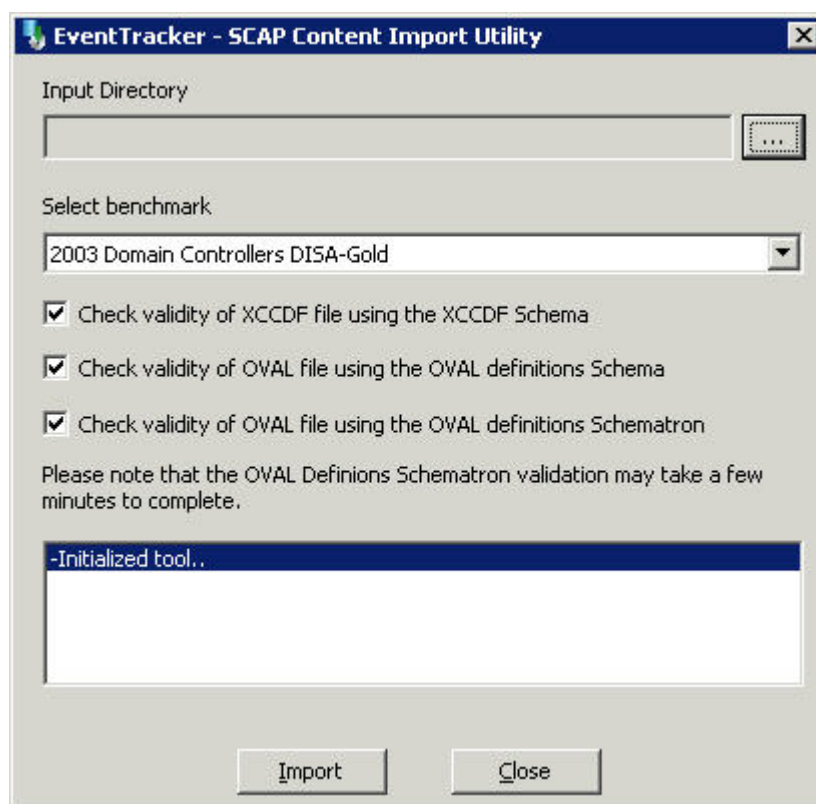
You cannot add a new Benchmark to the existing set of Benchmarks.


To import SCAP Benchmarks

- 1 Download the SCAP content from <http://web.nvd.nist.gov/view/ncp/repository> or some other source, unzip and save it in a safe location.
- 2 Open the Export Import Utility.
- 3 Click the **Import** tab.
- 4 Select the **SCAP** option.

EventTracker displays the SCAP Content Import Utility.

Figure 529
SCAP Content
Import Utility

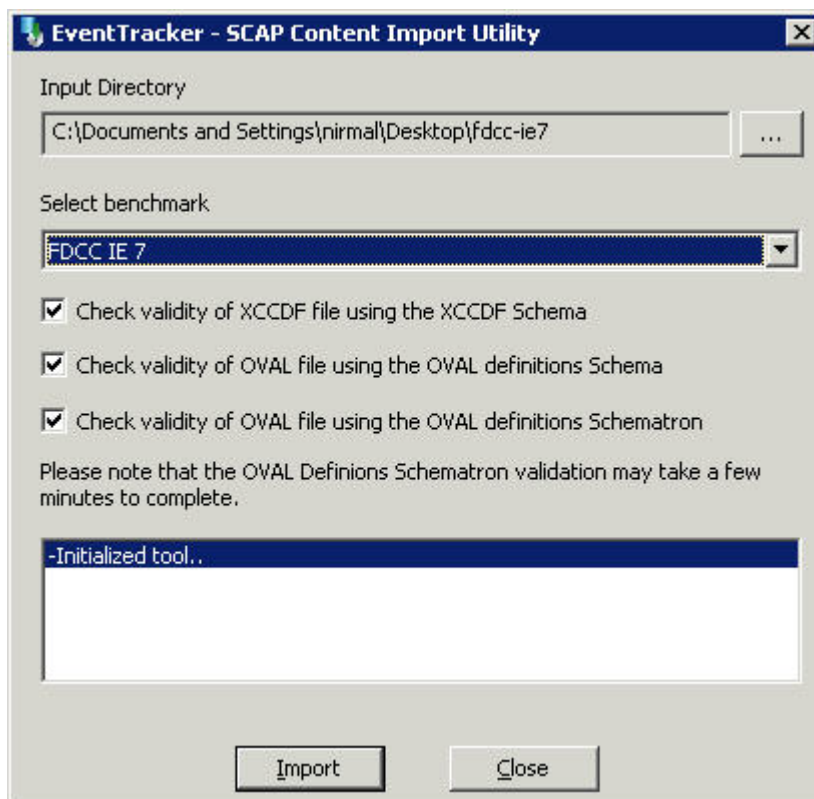


- 5 Click the browse button 

EventTracker displays the Browse For Folder window.
- 6 Navigate and locate the SCAP bundle that you want to import.

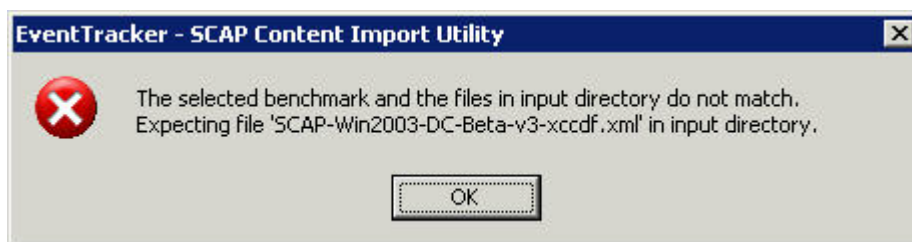
- 7 Click **OK**.
EventTracker updates the **Input Directory** field with the path of the SCAP bundle.
- 8 Select the Benchmark that you want to update from the **Select Benchmarks** drop-down list.

Figure 530
SCAP Content
Import Utility



SCAP Content Import Utility displays the error message if the selected benchmark and the files in the Input Directory do not match.

Figure 531
Incompatible
Benchmark



By default, SCAP Content Import Utility selects all three validation options.

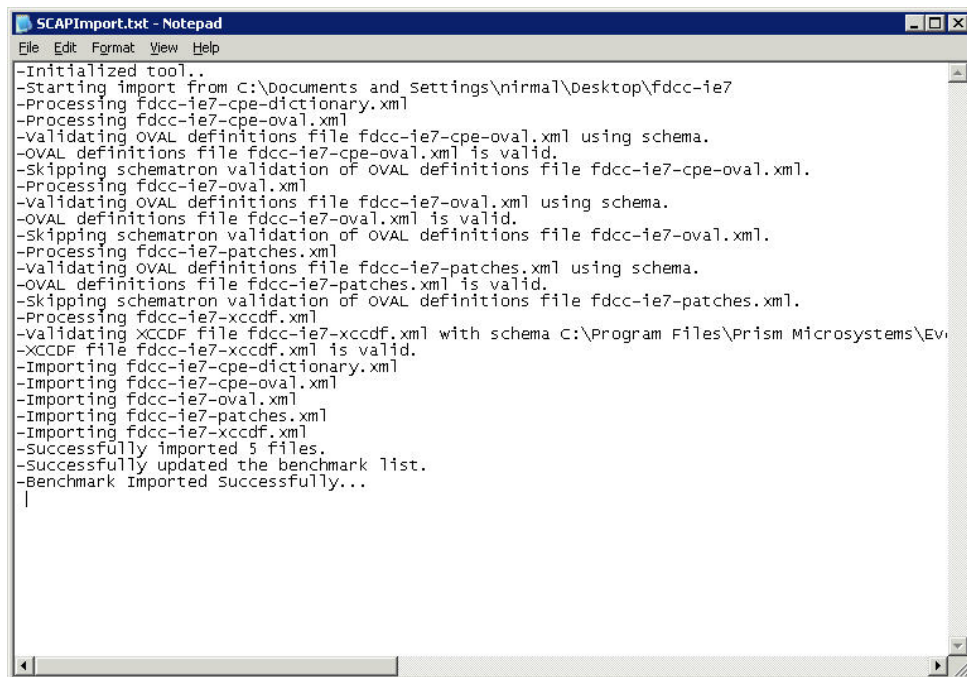
- 9 Clear the checkboxes as you deem fit.
- 10 Click **Import**.
If the validation is successful, SCAP Content Import Utility imports the Benchmark rules and displays the success message box.

Figure 532
Import - Success



Click **View Log** to view log in Notepad.

Figure 533
Successful Import
log



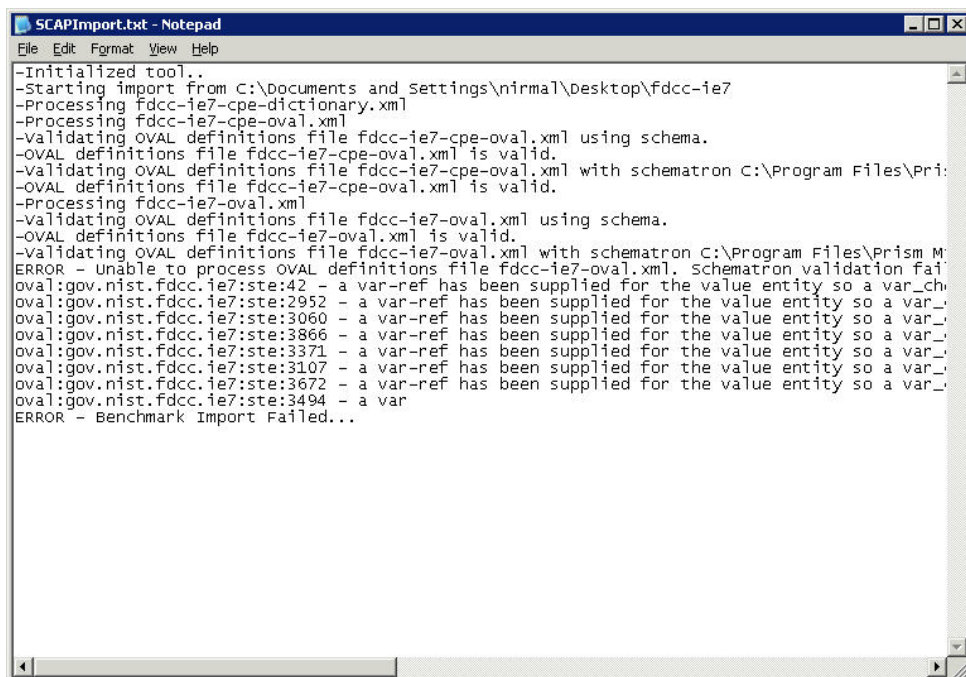
If the validation fails, SCAP Content Import Utility displays the failed message box and aborts the import operation.

Figure 534
Import - Failed



Click **View Log** to view log in Notepad.

Figure 535
Failed Import log



```

SCAPImport.txt - Notepad
File Edit Format View Help
-Initialized tool..
-Starting import from C:\documents and Settings\nirmal\Desktop\fdcc-ie7
-Processing fdcc-ie7-cpe-dictionary.xml
-Processing fdcc-ie7-cpe-oval.xml
-Validating OVAL definitions file fdcc-ie7-cpe-oval.xml using schema.
-OVAL definitions file fdcc-ie7-cpe-oval.xml is valid.
-Validating OVAL definitions file fdcc-ie7-cpe-oval.xml with schematron C:\Program Files\Prism M
-OVAL definitions file fdcc-ie7-cpe-oval.xml is valid.
-Processing fdcc-ie7-oval.xml
-Validating OVAL definitions file fdcc-ie7-oval.xml using schema.
-OVAL definitions file fdcc-ie7-oval.xml is valid.
-Validating OVAL definitions file fdcc-ie7-oval.xml with schematron C:\Program Files\Prism M
ERROR - Unable to process OVAL definitions file fdcc-ie7-oval.xml. schematron validation fai
oval:gov.nist.fdcc.ie7:ste:42 - a var-ref has been supplied for the value entity so a var_ch
oval:gov.nist.fdcc.ie7:ste:2952 - a var-ref has been supplied for the value entity so a var_
oval:gov.nist.fdcc.ie7:ste:3060 - a var-ref has been supplied for the value entity so a var_
oval:gov.nist.fdcc.ie7:ste:3866 - a var-ref has been supplied for the value entity so a var_
oval:gov.nist.fdcc.ie7:ste:3371 - a var-ref has been supplied for the value entity so a var_
oval:gov.nist.fdcc.ie7:ste:3107 - a var-ref has been supplied for the value entity so a var_
oval:gov.nist.fdcc.ie7:ste:3672 - a var-ref has been supplied for the value entity so a var_
oval:gov.nist.fdcc.ie7:ste:3494 - a var
ERROR - Benchmark Import Failed...

```

How To...

This section addresses very basic questions on how to use EventTracker generated Configuration Assessment results.

How to View Failed Config Assessment Results?

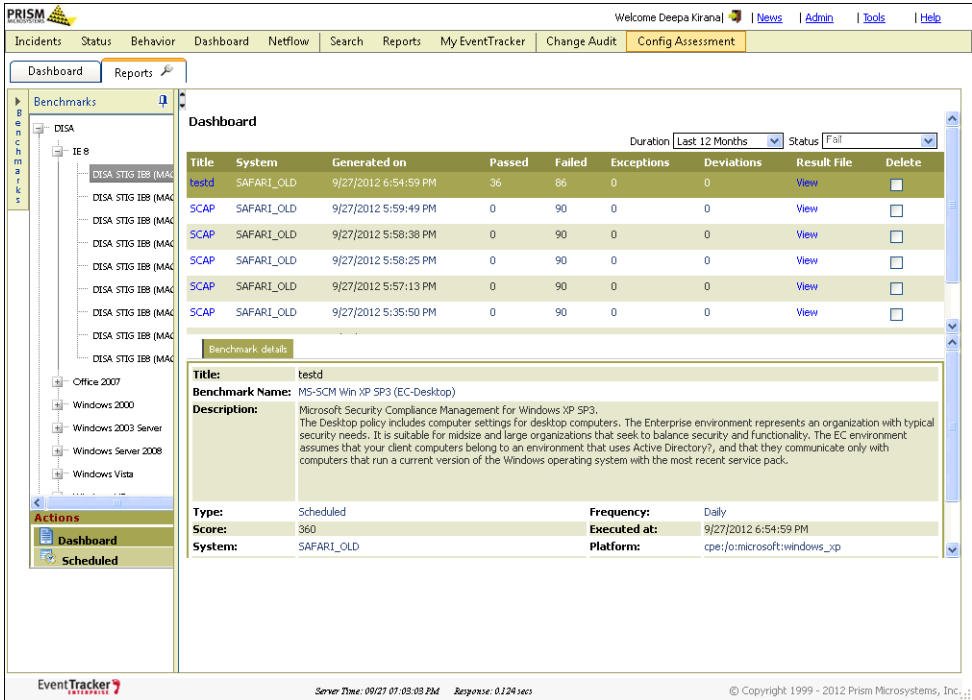
- 1 Log on to EventTracker Enterprise.
- 2 Click **Config Assessment**.
- 3 Click the **Reports** tab.

By default, EventTracker displays high-level summary of successful benchmark assessment results for the past 24 hours on the Dashboard.

You can select the duration ranging from 1 day to 12 months.

- 4 Select **Fail** from the **Status** drop-down list to view failed assessment attempts.
- EventTracker displays the summary of failed assessments with rationale why it failed.

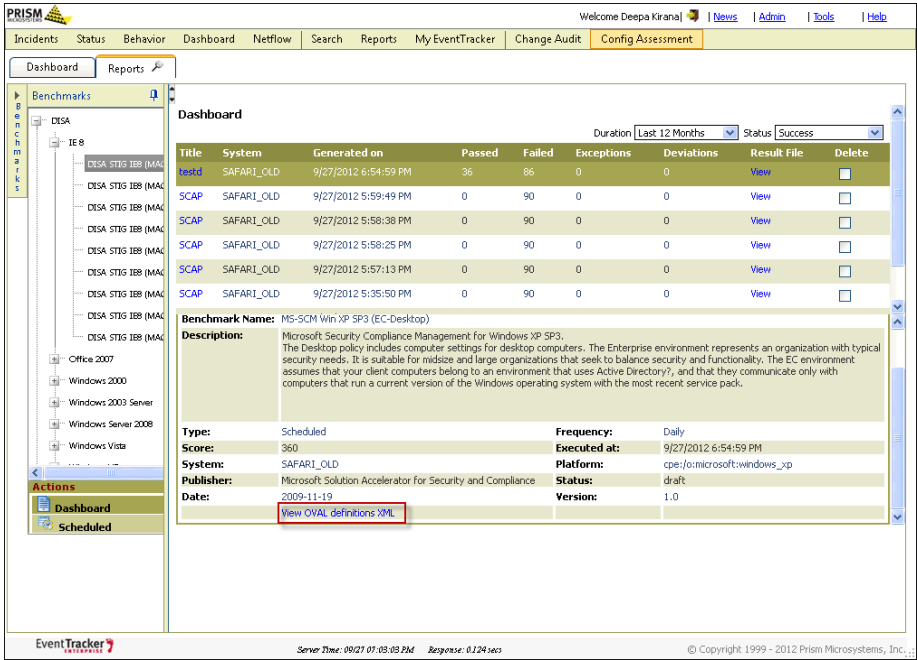
Figure 536
Config Assessment -
Failed



How to View OVAL Definitions?

- 1 Select **Success** or **Fail** from the **Status** drop-down list.
- 2 Scroll-down the Benchmark details pane.
- 3 Click the **View OVAL definitions XML** link.

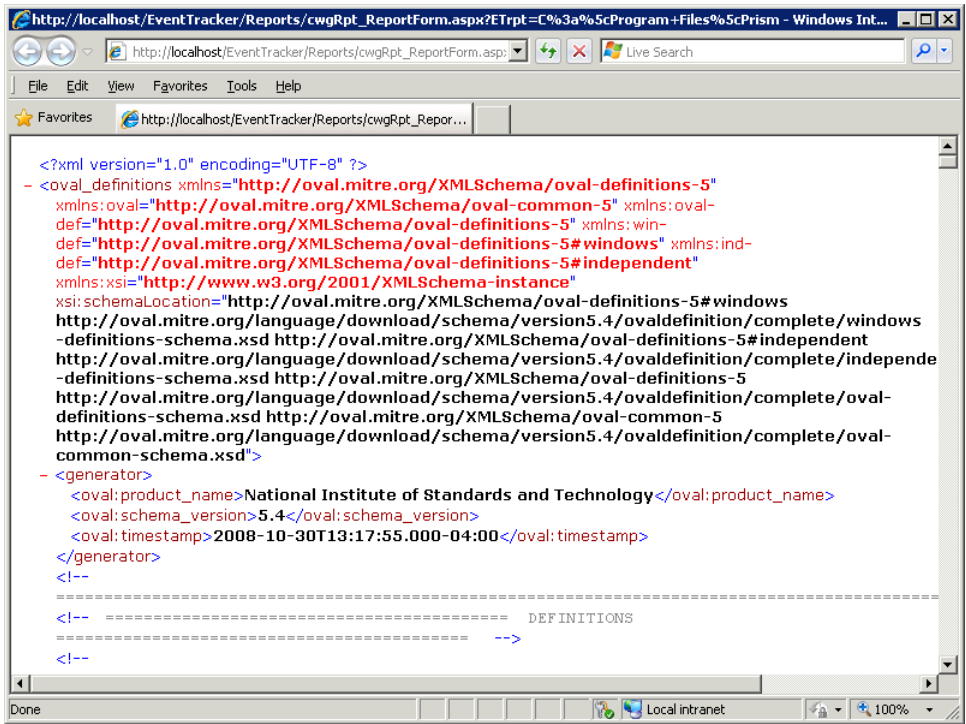
Figure 537
View OVAL
definitions



EventTracker displays the File Download pop-up window.

- 4 Click **Open** to view OVAL definitions.

Figure 538
OVAL definitions



How to View CCE Id of a Rule?

- 1 Select **Success** from the **Status** drop-down list.
- 2 Click the link in the **Title** column on the top pane.

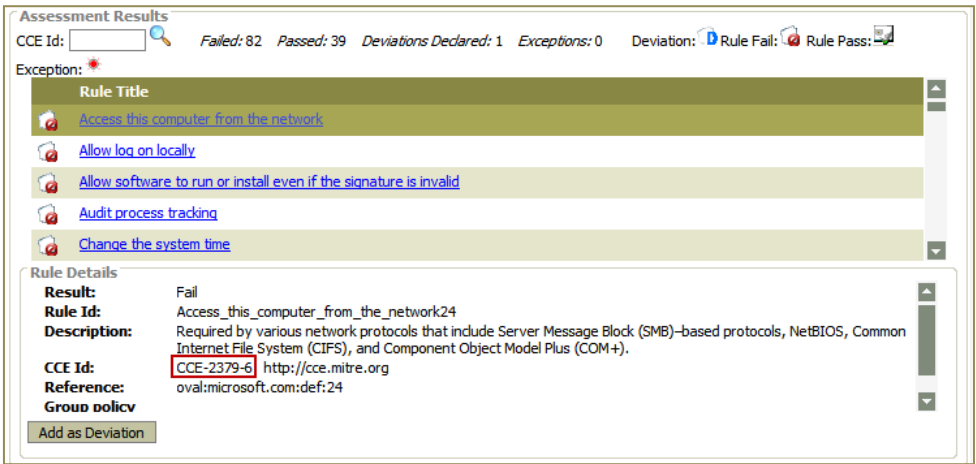
Note

EventTracker displays this link only for successful benchmark assessment.


EventTracker displays the **Config Assessment results** page.

- 3 Click a rule on the Assessment Results pane to view corresponding details on the Rule Details pane. Rule Details include CCE Id.

Figure 539
CCE Id



How to Locate a Rule Using CCE Id Search?

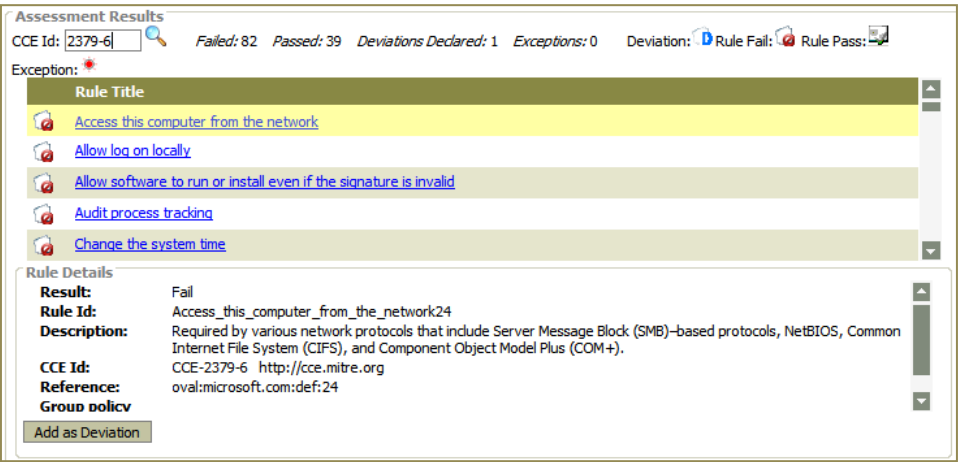
- 1 Type the CCE Id in the **CCE Id** field on the **Config Assessment results** page.
Example: CCE-2986-8
- 2 Click the search icon .

EventTracker displays the pop-up window with count of matches found and highlights the search result in yellow color.

Figure 540
Match count



Figure 541
Search result



3 Click the rule to view corresponding details.

How to View Status and Publication Date of a Benchmark?

- 1 Select **Success** or **Fail** from the **Status** drop-down list on the Dashboard.
- 2 Scroll-down the Benchmark details pane to view Status and Publication Date of the Benchmark.

Publication date specifies date at which the Benchmark attained the displayed status. Status includes any one of the following 'accepted', 'draft', 'interim', 'incomplete', and 'deprecated'.

Figure 542
Benchmark Status
and Publication date

Dashboard

Duration

Last 1 Day

Status

Success

Title	System	Generated on	Passed	Failed	Exceptions	Deviations	Result File	Delete
Test2	MCLOON	7/5/2011 4:06:17 PM	39	82	0	1	View	<input type="checkbox"/>
IE8	MCLOON	7/5/2011 4:06:11 PM	0	20	0	0	View	<input type="checkbox"/>
IE8	MCLOON	7/5/2011 4:05:56 PM	0	20	0	0	View	<input type="checkbox"/>
Test2	MCLOON	7/5/2011 4:03:34 PM	39	83	0	0	View	<input type="checkbox"/>
Test	MCLOON	7/5/2011 4:03:09 PM	39	83	0	0	View	<input type="checkbox"/>
Test2	MCLOON	7/5/2011 2:07:09 PM	39	83	0	0	View	<input type="checkbox"/>

Description:

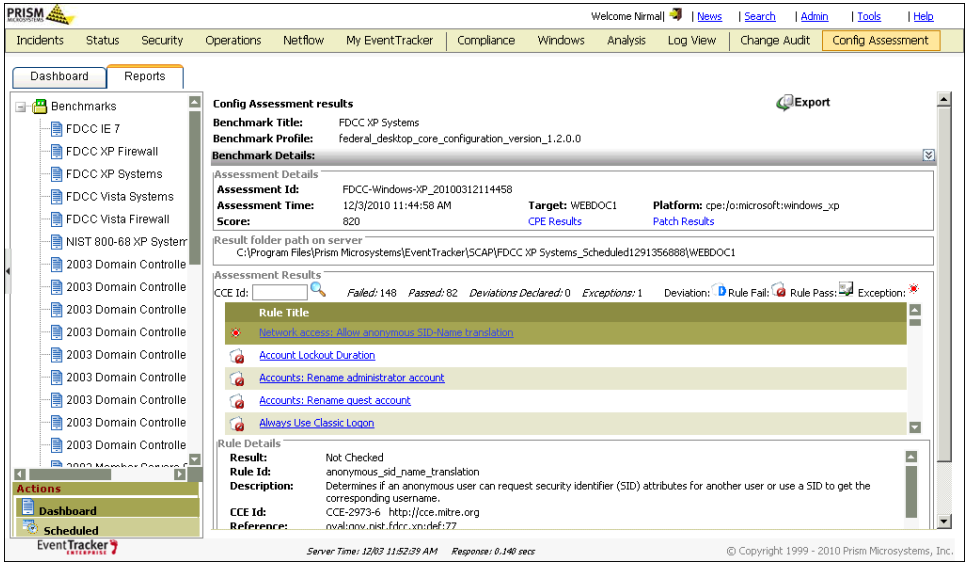
Microsoft Security Compliance Management for Windows XP SP3.
The Desktop policy includes computer settings for desktop computers. The Enterprise environment represents an organization with typical security needs. It is suitable for midsize and large organizations that seek to balance security and functionality. The EC environment assumes that your client computers belong to an environment that uses Active Directory?, and that they communicate only with computers that run a current version of the Windows operating system with the most recent service pack.

Type:	Scheduled	Frequency:	Daily
Score:	390	Executed at:	7/5/2011 4:06:17 PM
System:	MCLOON	Platform:	cpe:/o:microsoft:windows_xp
Publisher:	Microsoft Solution Accelerator for Security and Compliance	Status:	draft
Date:	2009-11-19	Version:	1.0
View OVAL definitions XML			

How to View Patch Results and CVE IDs?

- 1 Select **Success** from the Status drop-down list on the Dashboard.
- 2 Click the link in the **Title** column on the top pane.
EventTracker displays the Config Assessment results page.
- 3 Click the **Patch Results** link on the Benchmark Details pane.

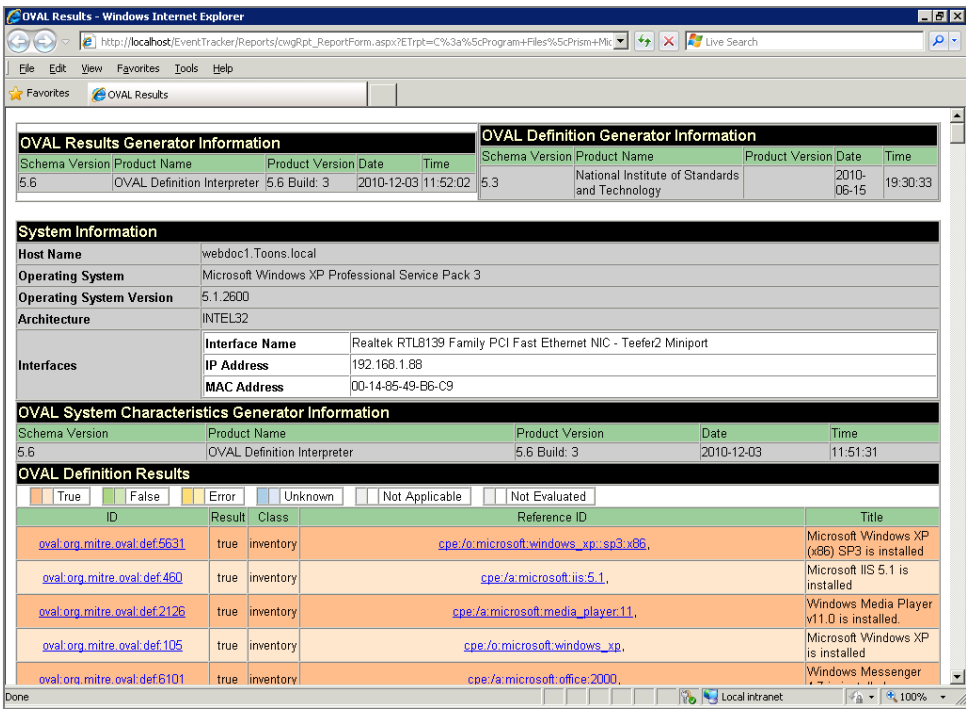
Figure 543
Patch Results



EventTracker displays the File Download pop-up window.

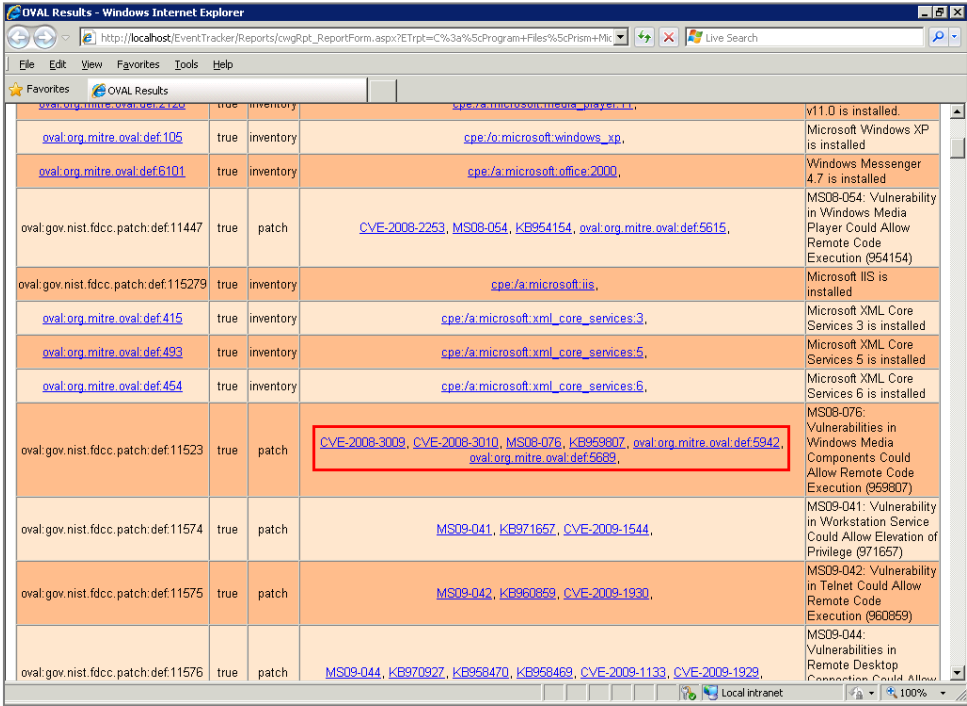
- 4 Click **Open** to view Patch Results.

Figure 544
Patch Results



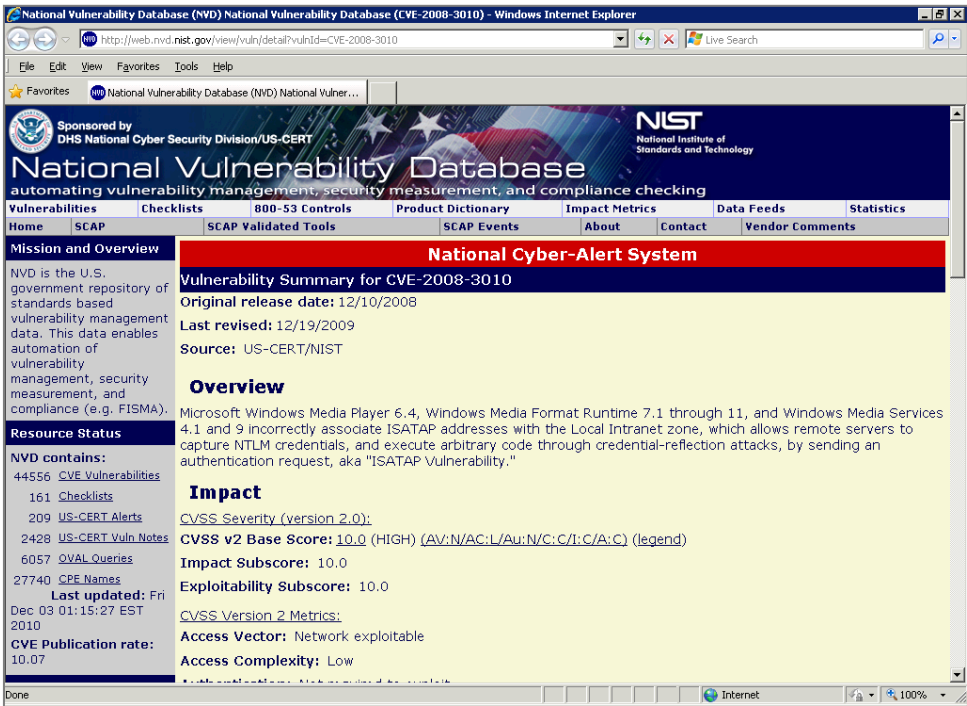
- 5 Click the hyperlinks under OVAL Definition Results -> Reference ID column to go to NVD page.

Figure 545
Patch Results



oval.org.mitre.oval.def.4146	true	inventory	cpe:/a:microsoft:windows_media_player-11,	V11.0 is installed.
oval.org.mitre.oval.def.105	true	inventory	cpe:/o:microsoft:windows_xp,	Microsoft Windows XP is installed
oval.org.mitre.oval.def.6101	true	inventory	cpe:/a:microsoft:office_2000,	Windows Messenger 4.7 is installed
oval.gov.nist.fdcc.patch.def.11447	true	patch	CVE-2008-2253 , MS08-054 , KB954154 , oval.org.mitre.oval.def.5615 ,	MS08-054: Vulnerability in Windows Media Player Could Allow Remote Code Execution (954154)
oval.gov.nist.fdcc.patch.def.115279	true	inventory	cpe:/a:microsoft:iis,	Microsoft IIS is installed
oval.org.mitre.oval.def.415	true	inventory	cpe:/a:microsoft.xml_core_services:3,	Microsoft XML Core Services 3 is installed
oval.org.mitre.oval.def.493	true	inventory	cpe:/a:microsoft.xml_core_services:5,	Microsoft XML Core Services 5 is installed
oval.org.mitre.oval.def.454	true	inventory	cpe:/a:microsoft.xml_core_services:6,	Microsoft XML Core Services 6 is installed
oval.gov.nist.fdcc.patch.def.11523	true	patch	CVE-2008-3009 , CVE-2008-3010 , MS08-076 , KB959807 , oval.org.mitre.oval.def.5942 , oval.org.mitre.oval.def.5669 ,	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)
oval.gov.nist.fdcc.patch.def.11574	true	patch	MS09-041 , KB971657 , CVE-2009-1544 ,	MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)
oval.gov.nist.fdcc.patch.def.11575	true	patch	MS09-042 , KB960859 , CVE-2009-1930 ,	MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution (960859)
oval.gov.nist.fdcc.patch.def.11576	true	patch	MS09-044 , KB970927 , KB958470 , KB958468 , CVE-2009-1133 , CVE-2009-1929 ,	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow

Figure 546
NVD page



National Vulnerability Database (NVD) National Vulnerability Database (CVE-2008-3010)

Sponsored by DHS National Cyber Security Division/US-CERT

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists 800-53 Controls Product Dictionary Impact Metrics Data Feeds Statistics

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 44556 CVE Vulnerabilities
- 161 Checklists
- 209 US-CERT Alerts
- 2428 US-CERT Vuln Notes
- 6057 OVAL Queries
- 27740 CPE Names

Last updated: Fri Dec 03 01:15:27 EST 2010

CVE Publication rate: 10.07

National Cyber-Alert System

Vulnerability Summary for CVE-2008-3010

Original release date: 12/10/2008

Last revised: 12/19/2009

Source: US-CERT/NIST

Overview

Microsoft Windows Media Player 6.4, Windows Media Format Runtime 7.1 through 11, and Windows Media Services 4.1 and 9 incorrectly associate ISATAP addresses with the Local Intranet zone, which allows remote servers to capture NTLM credentials, and execute arbitrary code through credential-reflection attacks, by sending an authentication request, aka "ISATAP Vulnerability."

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:I/C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

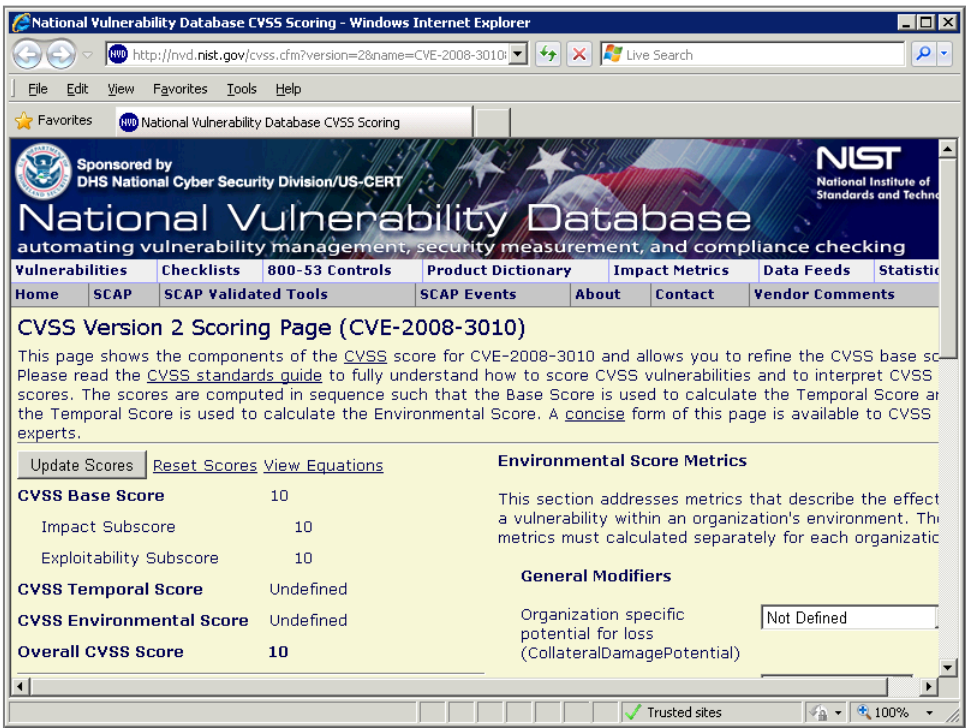
CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

6 Scroll down and click the CVSS v2 Base Score to go CVSS Version 2 Scoring Page.

Figure 547
NVD page



How to Verify XCCDF Content is not Applicable to a Platform?

- 1 Select a benchmark, for example, FDCC XP Systems to schedule Config Assessment against the managed computers.
- 2 In the Actions pane, click **Dashboard**.
- 3 Select **Fail** from the **Status** drop-down list.

EventTracker displays the summary of failed assessments with rationale why it failed.

Figure 548
Benchmark
incompatible to the
Platform

The screenshot displays the PRISM EventTracker 7.3 Enterprise web application. The top navigation bar includes links for Incidents, Status, Behavior, Dashboard, Netflow, Search, Reports, My EventTracker, Change Audit, and Config Assessment. The left sidebar shows a tree view of benchmarks, including DISA STIG IEB (MAC), Office 2007, and Windows 2000. The main content area is divided into two sections: a top pane showing a list of benchmarks and a bottom pane showing details for a selected benchmark.

Dashboard Table:

Title	System	Generated on	Passed	Failed	Exceptions	Deviations	Result File	Delete
testd	SAFARI_OLD	9/27/2012 6:54:59 PM	36	86	0	0	View	<input type="checkbox"/>
SCAP	SAFARI_OLD	9/27/2012 5:59:49 PM	0	90	0	0	View	<input type="checkbox"/>
SCAP	SAFARI_OLD	9/27/2012 5:58:38 PM	0	90	0	0	View	<input type="checkbox"/>
SCAP	SAFARI_OLD	9/27/2012 5:58:25 PM	0	90	0	0	View	<input type="checkbox"/>
SCAP	SAFARI_OLD	9/27/2012 5:57:13 PM	0	90	0	0	View	<input type="checkbox"/>
SCAP	SAFARI_OLD	9/27/2012 5:35:50 PM	0	90	0	0	View	<input type="checkbox"/>

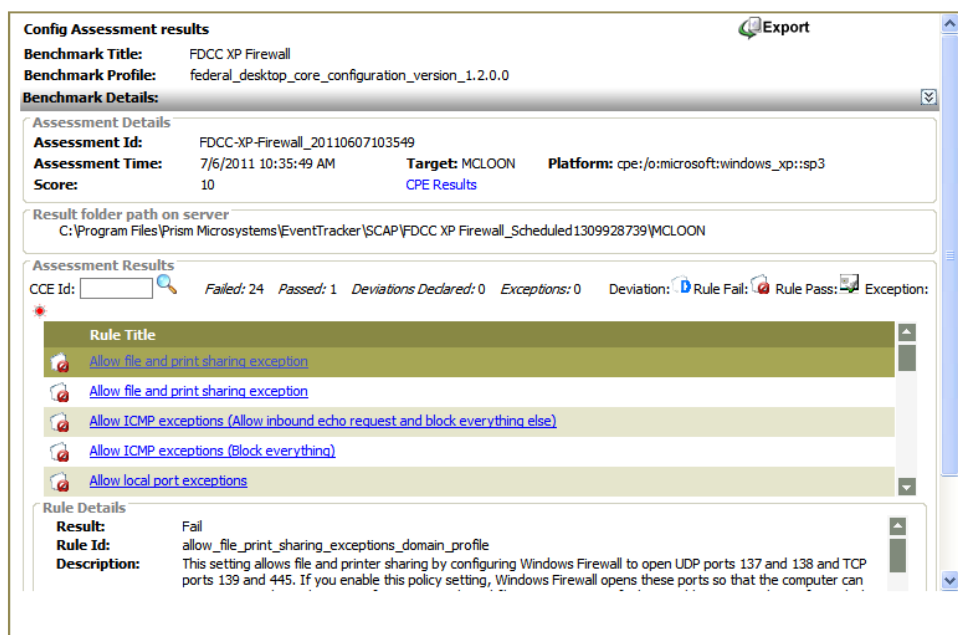
Benchmark details:

Title: testd
Benchmark Name: MS-SCM Win XP SP3 (EC-Desktop)
Description: Microsoft Security Compliance Management for Windows XP SP3. The Desktop policy includes computer settings for desktop computers. The Enterprise environment represents an organization with typical security needs. It is suitable for midsize and large organizations that seek to balance security and functionality. The EC environment assumes that your client computers belong to an environment that uses Active Directory?, and that they communicate only with computers that run a current version of the Windows operating system with the most recent service pack.
Type: Scheduled
Frequency: Daily
Score: 360
Executed at: 9/27/2012 6:54:59 PM
System: SAFARI_OLD
Platform: cpe:/o:microsoft:windows_xp

How to Locate the Config Assessment Result Folder on Server?

- 1 Select **Success** from the **Status** drop-down list.
 - 2 Click the link in the **Title** column on the top pane.
- EventTracker displays the Config Assessment results page.

Figure 549
Result Folder path



EventTracker stores the assessment results under the root directory `...\Program Files\Prism Microsystems\EventTracker\SCAP`.

Typical naming convention would be, root directory\title of the assessment schedule+Timeticks of when the report was generated\name of the system against which the assessment was done.

`...\Program Files\Prism Microsystems\EventTracker\SCAP\FDCC XP Systems_Scheduled1288692581\WEBDOC1`

Config Assessment Dashboard

Configuration Assessment Dashboard allows you to add Dashlets to view itemized Config Assessment Results.

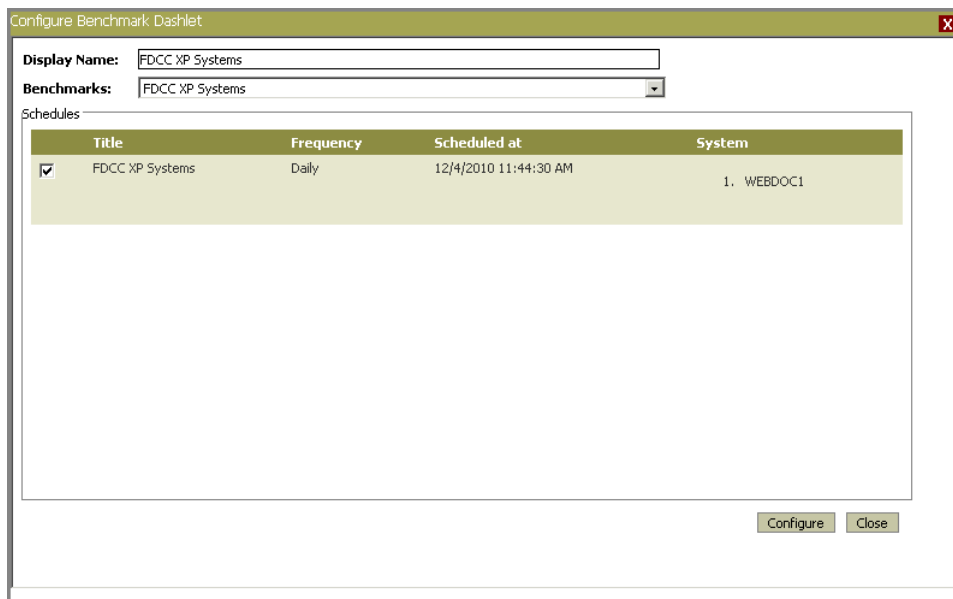
To view Change Audit Dashboard

- 1 Click **Config Assessment**.
- 2 Move the mouse pointer over Dashboard.
- 3 From the dropdown list, click the **Configure** hyperlink.
EventTracker displays the **Configure Benchmark Dashlet** pop-up window.
- 4 Type a comprehensible name in the **Display Name** field.
- 5 Select a policy from the **Policy Name** drop-down list.

EventTracker displays the Configure Benchmark Dashlet pop-up window with Schedule details of the selected Policy.

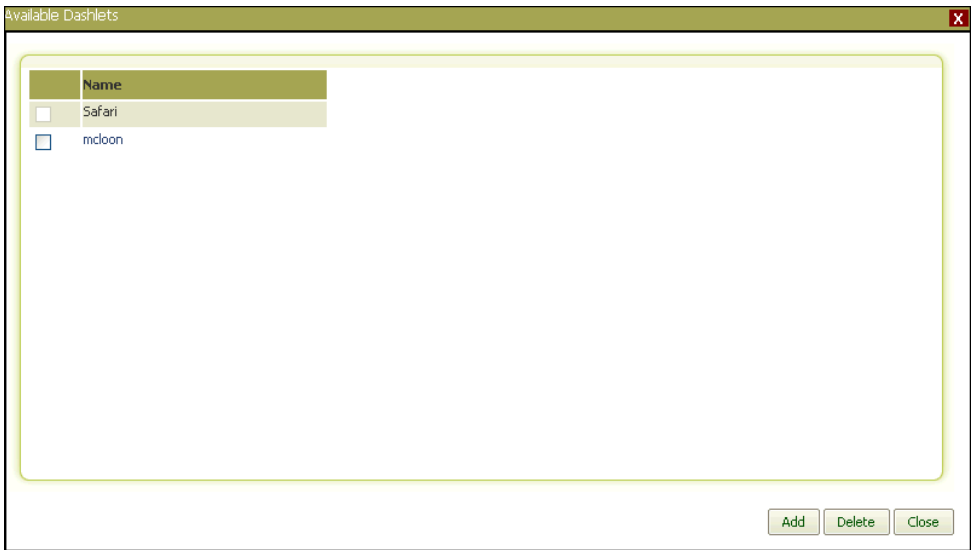
- 6 Select the Schedule(s).

Figure 550
Configure
Benchmark Dashlet



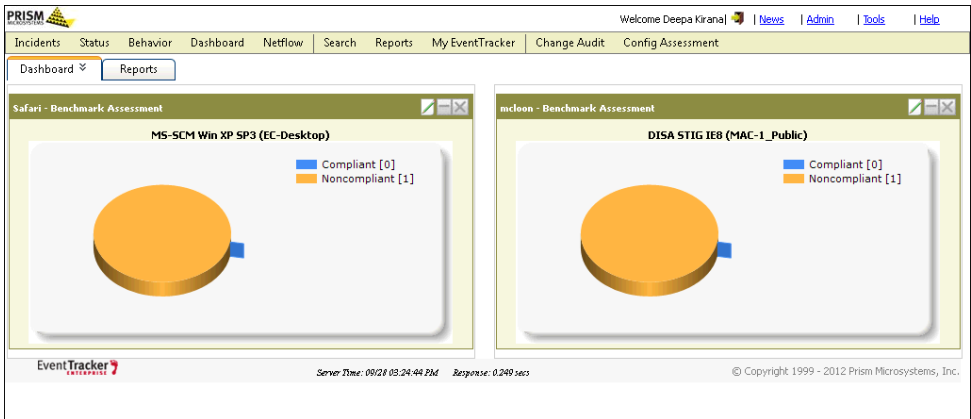
- 7 Click **Configure**.
 - 8 Move the mouse pointer over Dashboard.
 - 9 Click the **Customize** hyperlink.
- EventTracker displays the **Available Dashlets** pop-up window.

Figure 551
Available Dashlets



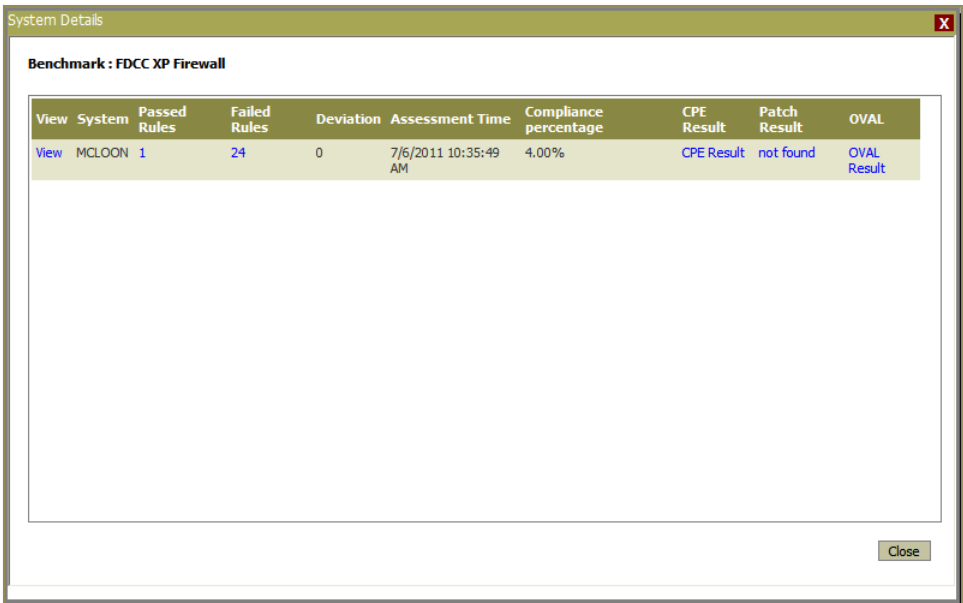
- 10 Select the Dashlet(s) and then click **Add**.
EventTracker displays the Dashboard with newly added Dashlet(s).

Figure 552
Available Dashlets



- 11 Click a graph or a legend to view respective System Details.

Figure 553
System Details

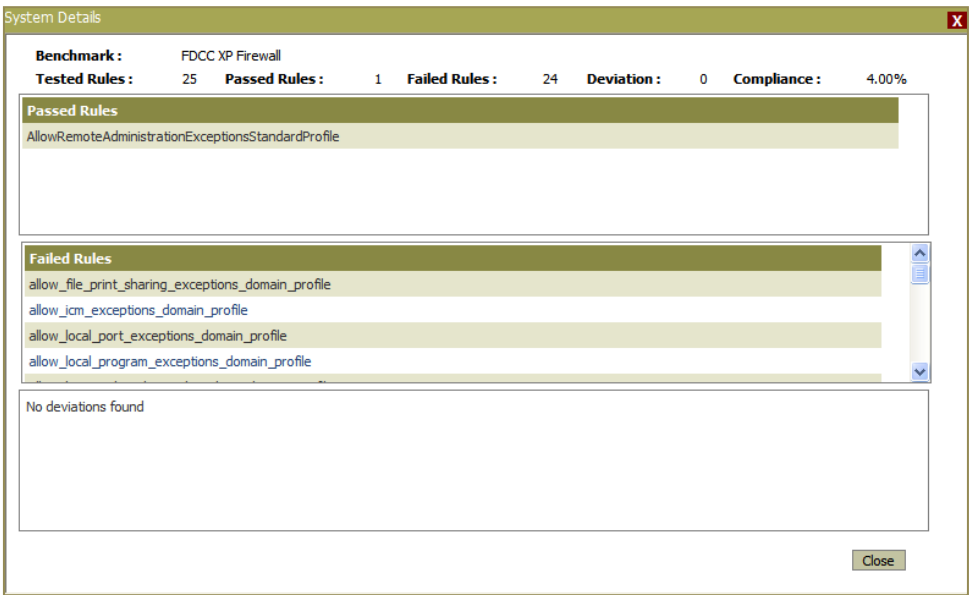


The screenshot shows a window titled 'System Details' with a close button (X) in the top right corner. Inside the window, the title 'Benchmark : FDCC XP Firewall' is displayed. Below this is a table with the following columns: View, System, Passed Rules, Failed Rules, Deviation, Assessment Time, Compliance percentage, CPE Result, Patch Result, and OVAL. The first row of data shows 'View' as a hyperlink, 'System' as 'MCLOON', 'Passed Rules' as '1', 'Failed Rules' as '24', 'Deviation' as '0', 'Assessment Time' as '7/6/2011 10:35:49 AM', 'Compliance percentage' as '4.00%', 'CPE Result' as 'CPE Result', 'Patch Result' as 'not found', and 'OVAL' as 'OVAL Result'. A 'Close' button is located at the bottom right of the window.

View	System	Passed Rules	Failed Rules	Deviation	Assessment Time	Compliance percentage	CPE Result	Patch Result	OVAL
View	MCLOON	1	24	0	7/6/2011 10:35:49 AM	4.00%	CPE Result	not found	OVAL Result

- 12 Click the **View** hyperlink in the to view configuration assessment details.
- 13 Click the hyperlink in the **Passed Rules** column to view Benchmark rules that found to comply/failed to comply.

Figure 554
System Details



The screenshot shows the 'System Details' window with detailed benchmark results for 'FDCC XP Firewall'. At the top, it displays 'Benchmark : FDCC XP Firewall' and a summary: 'Tested Rules : 25', 'Passed Rules : 1', 'Failed Rules : 24', 'Deviation : 0', and 'Compliance : 4.00%'. Below this, there are three sections: 'Passed Rules' (containing 'AllowRemoteAdministrationExceptionsStandardProfile'), 'Failed Rules' (containing 'allow_file_print_sharing_exceptions_domain_profile', 'allow_icm_exceptions_domain_profile', 'allow_local_port_exceptions_domain_profile', and 'allow_local_program_exceptions_domain_profile'), and 'No deviations found'. A 'Close' button is at the bottom right.

Benchmark : FDCC XP Firewall	
Tested Rules :	25
Passed Rules :	1
Failed Rules :	24
Deviation :	0
Compliance :	4.00%

Passed Rules

- AllowRemoteAdministrationExceptionsStandardProfile

Failed Rules

- allow_file_print_sharing_exceptions_domain_profile
- allow_icm_exceptions_domain_profile
- allow_local_port_exceptions_domain_profile
- allow_local_program_exceptions_domain_profile

No deviations found

- 14 Click the hyperlink in the **Failed Rules** column to view Benchmark rules that failed to comply/found to comply.
- 15 Click the hyperlink in the **CPE Result** column to view CPE OVAL result.
- 16 Click the hyperlink in the **Patch Result** column to view CPE Patch result.
- 17 Click the hyperlink in the **OVAL** column to view OVAL XML report.

Chapter 27

Tag Cloud Weighting

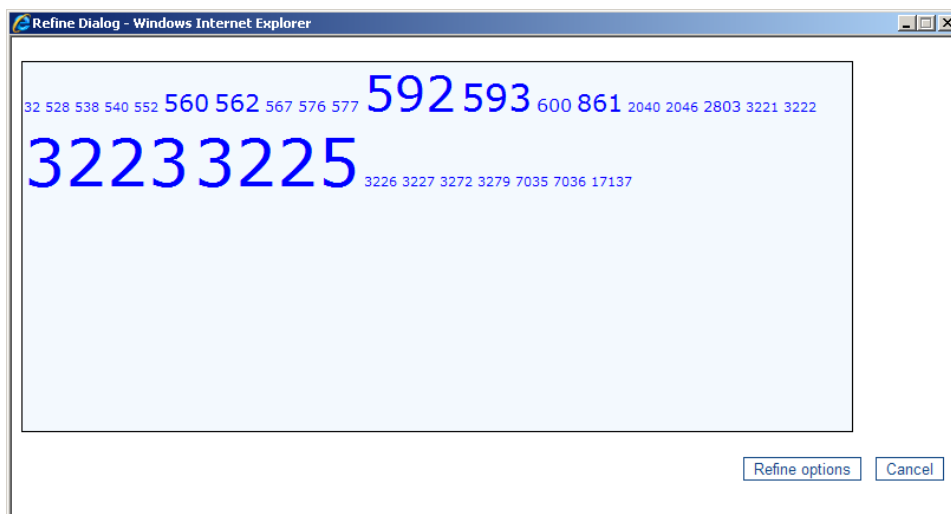
In this chapter, you will learn how to:

- [Assign Weights to Tags](#)
- [Add Keywords as Tags](#)

Tag Clouds

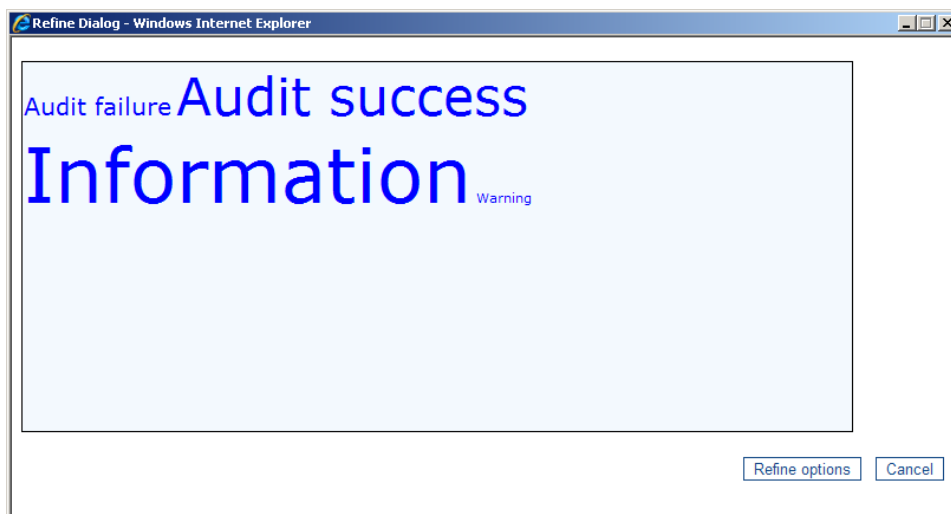
A tag cloud is a set of related tags with corresponding weights. The weights are represented using font sizes or other visual clues.

Figure 555
Tag Cloud



Tag clouds are interactive: tags are hyperlinks typically allowing the user to drill down on the data. Tag clouds display order is generally alphabetical.

Figure 556
Tag Cloud



When the search is over, EventTracker Log Search browser displays the Tag menu in the Menu bar, which in turn has options to refine the query result.

Figure 557
Show Refined Data
window

Logtime	Event ID	Event Type	Category	Event ID	Source	Domain	LogType	Event source	Event description
9/5/2011 11:59:54 AM	593	NT AUTHORITY	Security	Security					A process has exited: Process ID: 2248 Image File Name: C:\Program Files\Prim Microsystems\EventTracker\evProcessEFile.exe User Name: MCLOONS Domain: TOONS Logon ID: (0x0,0x3E7)
9/5/2011 11:59:54 AM	592	NT AUTHORITY	Security	Security					A new process has been created: New Process ID: 4304 Image File Name: C:\Program Files\Prim Microsystems\EventTracker\AdvancedReports\Prim.EventTracker.Reporter.exe Creator Process ID: 964 User Name: MCLOONS Domain: TOONS Logon ID: (0x0,0x3E7)
9/5/2011 11:59:53 AM	592	SYSTEM	MCLOON	NT AUTHORITY	Security	Security			A new process has been created: New Process ID: 5064 Image File Name: C:\WINDOWS\system32\net1.exe Creator Process ID: 1760 User Name: MCLOONS Domain: TOONS Logon ID: (0x0,0x3E7)
9/5/2011 11:59:53 AM	592	SYSTEM	MCLOON	NT AUTHORITY	Security	Security			A new process has been created: New Process ID: 1760 Image File Name: C:\WINDOWS\system32\net.exe Creator Process ID: 6112 User Name: MCLOONS Domain: TOONS Logon ID: (0x0,0x3E7)
9/5/2011 11:59:53 AM	593	SYSTEM	MCLOON	NT AUTHORITY	Security	Security			A process has exited: Process ID: 4332 Image File Name: C:\WINDOWS\system32\net.exe User Name: MCLOONS Domain: TOONS Logon ID: (0x0,0x3E7)
9/5/2011 11:59:53 AM	593	SYSTEM	MCLOON	NT AUTHORITY	Security	Security			A process has exited: Process ID: 5024 Image File Name: C:\WINDOWS\system32\net1.exe

Search results for: Categories=*Security: Audit success* AND Time range=9/2/2011 12:23:40 PM - 9/5/2011 12:23:40 PM

Assigning Weights to Tags

This option helps to assign weights to tags.

To assign weights to tags

- 1 Log on to EventTracker Enterprise.
- 2 Click the **Admin** dropdown, and then click **Weights**.
EventTracker displays the **Weight configuration** page.

Figure 558
Weight
Configuration

Weight configuration

View configuration for:

Event Type

Assign weight

Event Type

Search:

Go

Page Size : 25

Name	Weight	
Edit Warning	Medium	<input type="checkbox"/>
Edit Verbose	Low	<input type="checkbox"/>
Edit Success	Low	<input type="checkbox"/>
Edit Information	Low	<input type="checkbox"/>
Edit Error	Serious	<input type="checkbox"/>
Edit Critical	Serious	<input type="checkbox"/>
Edit Audit Success	Low	<input type="checkbox"/>
Edit Audit Failure	High	<input type="checkbox"/>

Assign Multiple

- 3
- Select an option from the **View configuration for** drop-down list.
EventTracker displays the Weight configuration page with corresponding details.
- 4
- Click **Edit** against the tag you wish to reassign the Weight.

Figure 559

Weight configuration

View configuration for:

Event Type

Assign weight

Event Type

Search:

Go

Page Size : 25

Name	Weight	
Edit Warning	Medium	<input type="checkbox"/>
Edit Verbose	Low	<input type="checkbox"/>
Edit Success	Low	<input type="checkbox"/>
Update Cancel Information	<div>Low</div>	<input type="checkbox"/>
Edit Error	Serious	<input type="checkbox"/>
Edit Critical	Serious	<input type="checkbox"/>
Edit Audit Success	Low	<input type="checkbox"/>
Edit Audit Failure	High	<input type="checkbox"/>

Assign Multiple

- 5
- Select an appropriate option from the drop-down list in the **Weight** column.
- 6
- Click **Update**.
EventTracker updates the Tag with newly assigned weight.

Assigning Weights to Multiple Tags

This option helps you assign weights to multiple tags.

To assign weights to multiple tags

- 1 Select the checkbox against the tags you wish to assign weights.
- 2 Click **Assign Multiple**.

EventTracker displays the Assign Weight pop-up window.

Figure 560
Assign Weight

The image shows a pop-up window titled "Assign Weight". It has a green header bar. Below the header, there is a label "Weightage" followed by a dropdown menu currently showing "Undefined". At the bottom of the window, there are two buttons: "Assign" and "Cancel".

- 3 Select an option from the **Weightage** drop-down list.
- 4 Click **Assign**.

EventTracker assigns weights to the selected tags.

Adding Keywords as Tags

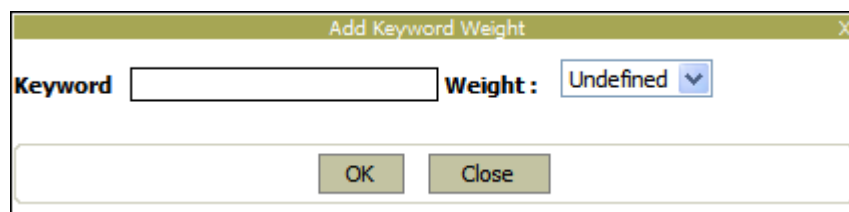
This option helps to add keywords as tags.

To add keywords

- 1 Select **Keyword** from the **View configuration** for drop-down list.
- 2 Click **Add new**.

EventTracker displays the Add Keyword Weight pop-up window.

Figure 561 Add
Keyword Weight

The image shows a pop-up window titled "Add Keyword Weight" with a close button (X) in the top right corner. It has a green header bar. Below the header, there is a label "Keyword" followed by a text input field. To the right of the input field is a label "Weight:" followed by a dropdown menu currently showing "Undefined". At the bottom of the window, there are two buttons: "OK" and "Close".

- 3 Type keyword in the **Keyword** field. Example: HardwareEvents
- 4 Select an option from the **Weight** drop-down list.
- 5 Click OK.

Chapter 28

Searching Logs

In this chapter, you will learn about:

- [Indexing Keywords](#)
- [Basic Search](#)
- [Advanced Search](#)

Searching Logs

EventTracker LogSearch is Google like search facility available for quick search of events, it supports simple string search to parameterized search. For more information, refer [EventTracker 7.0 Enterprise Log Search](#) guide.

How Indexing Works in Tandem with Log Search?

Keywords are unique words or short phrases used to make searching easier. To make the most of this feature, you must know the unique Keyword associated with the logs.

CAB files should be there in the server for the Keyword Indexer to index.

By default, Keyword Indexer

- 1 Indexes all unique words present in the CAB files that are generated in the past 24 hours. Keywords include unique words found in Event Properties (Standard Columns) and Description (Custom columns).
- 2 Displays match count versus day chart for the past 7 days data, for the indexed CAB files might contain data for the past 7 days.

Keyword Indexer maintains a master history file (History.xml) for the CAB files that are indexed and for each CAB file maintains an XML file (etar1271127929-14505.cab.xml) that contains a list of unique words indexed along with the count. All these files are stored in the default EventTracker installation path (...<Install path>\EventTracker\Archives\<port>\<year>\<month>\index\<CabName>.Xml).

When you present a query, Log Search Utility first consults the XML files; if the data searched for is present in the indexed CAB files, then it returns the result set. If the data searched for is not in the indexed CAB files, then it searches the unindexed CAB files and returns the result set. This way Keyword Indexer speeds up the search and find process to a great extent.

In the result set, selection option is provided for columns and values of Event Properties and Event Description to refine the result or to frame a new search query.

Key Features

- Immediate match counts for search string
- Current day tree view
- Last seven days match counts in graph view

Pros

- Faster log search. It improves the performance significantly. Performance measurement depends upon search string also. on an avg it can vary from 20% to 500%
- If Indexer is enabled, first page is displayed approximately within fifteen secs

Cons

- Indexing cab file is a resource intensive task. It will take minimum 40 - 50% of CPU usage and minimum 50-60 MB of memory usage

Benchmark Report on Keyword Indexer

Configuration Details

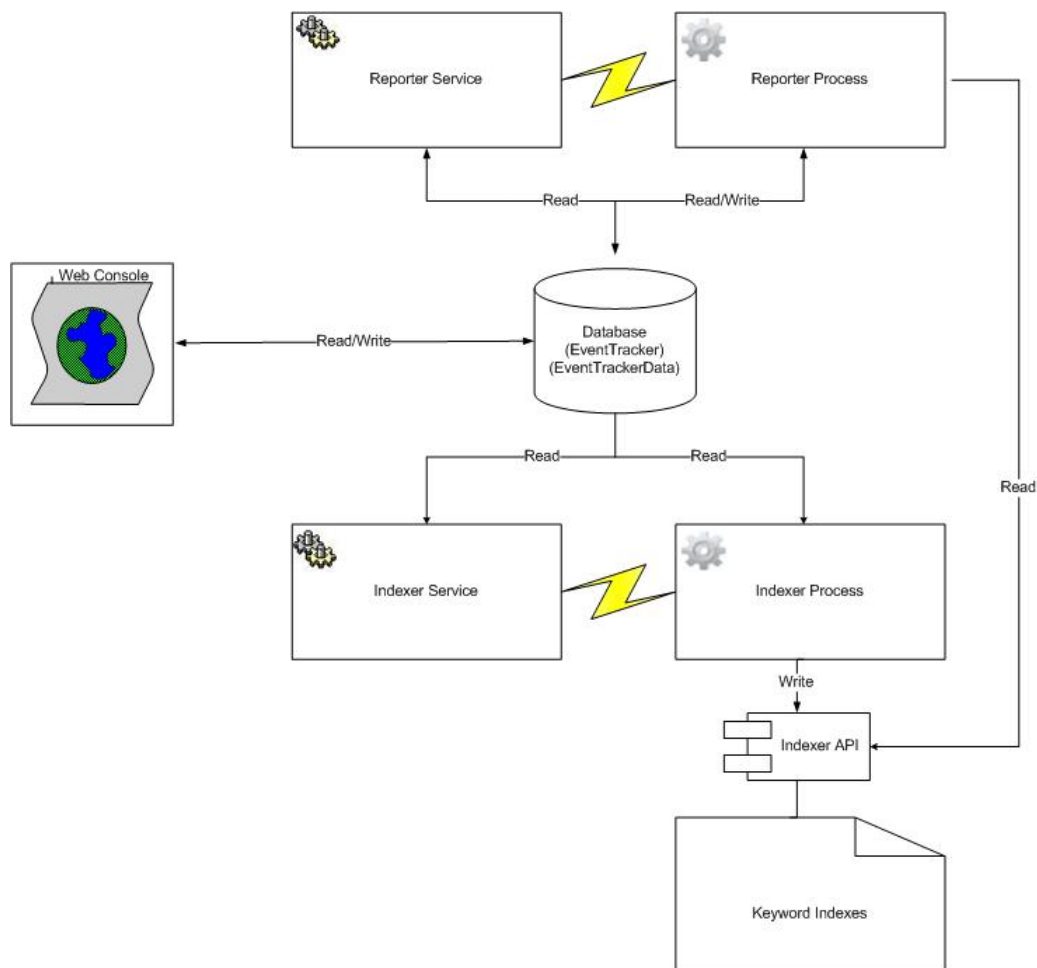
System: esxwin2k3vm3
From Time: 7/4/2009 9:34:24 PM
To Time: 9/22/2009 12:44:15 PM
Total Cabs: 300

Table 151

Search String	Match Count	Keyword Indexer Search	Log Search
SeNetworkLog onRight	250	First Page Processing Time = 7 sec Total Processing Time = 20 sec	First Page Processing Time = 5 mins 15 sec Total Processing Time = 11 min
560	1,18,257	First Page Processing Time = 8 sec Total Processing Time = 57 sec	First Page Processing Time = 34 sec Total Processing Time = 12 min
pkey	1	First Page Processing Time = 7 sec Total Processing Time = 7 sec	First Page Processing Time = 11 min (after 90%) Total Processing Time = 12 min
maryland	0	Not Required	Total Processing Time = 12 min.
susan	3,499,042	First Page Processing Time = 7 sec Total Processing Time = 46 sec (processing cancelled because report data exceeds the maximum limit)	First Page Processing Time = 20 sec Total Processing Time = 10+ min (processing cancelled because report data exceeds the maximum limit)

Keyword Indexer Overview

Figure 562
Keyword Indexer
Overview



Basic Search

Basic Search is an ideal way to search a word or phrase related to the information you are looking for. The search is done through Event Properties (standard columns) and Event Description (custom columns).

Advanced Search

Advanced Search offers numerous options for making your searches more precise and getting more useful results.

Chapter 29

Securing EventTracker

In this chapter, you will learn how to:

- [Harden Windows 2003/2008](#)
- [Use https to reach the EventTracker Console](#)
- [Enable Encryption from the Agent](#)
- [Enable Encryption from CP to CM](#)

Server Hardening

Server hardening consists of creating a baseline for the security on your servers in your organization. The default configurations of a Windows Server 2003/2008 computer are not designed with security as the primary focus. To protect your servers, you must establish solid and sophisticated security policies for all types of servers in your organization.

Windows Server 2003 Security Baseline:

<http://technet.microsoft.com/en-us/library/cc163140.aspx>

Windows Server 2008 Security Baseline:

<http://technet.microsoft.com/en-us/library/cc514539.aspx>

Securing Internet Information Services 6.0:

<http://technet.microsoft.com/en-us/library/cc875829.aspx>

Securing IIS Web Server with SSL:

<http://www.prismmicrosys.com/Support/latest%20guides/Securing%20IIS%20Web%20Server%20with%20SSL.pdf>

Encryption

To encrypt data in motion, EventTracker v7.3 Enterprise engine uses Microsoft's CAPI with "Microsoft Enhanced Cryptographic Provider" (RSAENH) and FIPS compliant cryptographic algorithms, Triple-DES (FIPS 46-3) and SHA1 (FIPS 180-3).

The FIPS compliance FIPS 140-2 or FIPS 140-1 depends on the OS as described in the following URL. See Microsoft's page about FIPS compliance:

<http://technet.microsoft.com/en-us/library/cc750357.aspx>

NIST page

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

The Federal Information Processing Standard (FIPS) Publication 140-2, FIPS PUB 140-2, is a U.S. government computer security standard used to accredit cryptographic modules.

Source: http://en.wikipedia.org/wiki/FIPS_140-2

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

<http://csrc.nist.gov/groups/STM/cmvp/>

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp720.pdf>

<http://technet.microsoft.com/en-us/library/cc180745.aspx>

Enabling Encryption from the Agent

This option helps you configure EventTracker Windows Agent to securely transfer files over the IP. For more information, refer Transferring Log Files section.

Enabling Encryption from CP to CM

This option helps you configure Collection Point to securely transfer files over the IP to Collection Master. For more information, refer Adding Collection Masters section.

Using https to Reach the EventTracker Console

Refer [Securing IIS Web Server with SSL.pdf](#) to provide secure access to EventTracker Web.

Chapter 30

Add-in Software Modules

In this chapter, you will learn about:

- [Trap Tracker](#)
- [Status Tracker](#)
- [Solaris Agent](#)

TrapTracker

TrapTracker is an integral component of EventTracker, which helps you monitor and manage critical traps emitted by network devices.

TrapTracker for Windows (TTW) consists of 2 components, the TTW Manager and a built-in MIB Compiler/Browser.

TTW Manager is the heart of the architecture. You should install the TTW Manager on the system where you require all SNMP Traps to be monitored. You can configure Alerts and Trap Severity. Alerts include E-mail, beep, console message and other custom notifications.

MIB Compiler/Browser is provided to compile Custom MIBS into the TTW system.

TrapTracker for Windows (TTW) console consists of the following options:

- **Alerts:** After the installation is completed, you can configure TTW to send you alerts, based on the type of events that are received. The types of Alerts supported are E-mail, beep, console message, and custom action.
 - **Multiple Window View:** Displays multiple windows to view a distinct set of events. You can set the selection criteria for viewing events.
-

StatusTracker

This tool helps you monitor the status of your IT resources and provides you various reports. You can make decisions based on the reports, to enhance the availability of your critical IT resources.

The StatusTracker console consists of the following options:

- **Managing Resources:** You can add resources through Web site, FTP Site, Manually, and IP Subnet. You can also modify and delete the existing resources.
 - **Managing Groups:** You can create a group for the selected resources. You can also modify and delete the existing group.
 - **Reporting:** You can generate the report on Application resources and system resources.
-

Solaris Agent

EventTracker for Solaris C-2 provides administrators with a monitoring and reporting interface that provides one the most information rich sources of audit information from the UNIX kernel. Using the Basic Security Module (BSM), the system administrator now has access to kernel auditing events. Audit logs can be extremely valuable for operations, security, and auditors alike. EventTracker manages the central repository of log data events needed for proper incident investigation or to meet regulatory compliance. The platform provides insights into the actions and behaviors of users and systems. This information can be used to detect insider threats, security violations, and other dangerous behavior patterns.

Benefits of Solaris Agent

- Convert BSM binary data into meaningful events
- Real-time user-defined alerts
- Event Correlation engine
- Secure event archival
- Access to EventTracker database and EventVault for reporting

Purchase

To purchase Solaris Agent, contact us by E-mail at sales@prismmicrosys.com

Appendix – HIPAA

HIPAA Compliance Reports

The Health Insurance Portability And Accountability (HIPAA) regulation impacts those in healthcare that exchange patient information electronically. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use or disclosure of the information.

As part of the requirements, HIPAA states that a security management process must exist in order to protect against 'attempted or successful unauthorized access, use, disclosure, modification or modification with system operations.' The organization must be able to monitor, report and alert on attempted or successful access to systems and application that contain sensitive patient information.

EventTracker provides the following reports to help comply with the HIPAA regulations:

User Logon report

HIPAA requirements (164.308 (a)(5) – log-in/log-out monitoring) states that user accesses to the system be recorded and monitored for possible abuse.

User Logoff report

HIPAA requirements clearly states that user accesses to the system be recorded and monitored for possible abuse. Remember, this intent is not just to catch hackers but also to document the accesses to medical details by legitimate users. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera in a parking lot.

Logon Failure report

The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

HIPAA requirements (164.308 (a)(3) – review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

Appendix – SOX

Sarbanes – Oxley Compliance Reports

Section 404 of the Sarbanes – Oxley (SOX) act describes specific regulations requires for publicly traded companies to document the management's 'Assessment of Internal Controls' over security processes.

The standard requires that a security management process must exist in order to protect against attempted or successful unauthorized access, use, disclosure, modification or interference with system operations. In other words, being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive financial information.

EventTracker provides the following reports to help comply with the SOX regulations:

User Logoff report

SOX requirements (Sec 302 (a)(4)(C) and (D) states that user accesses to the system be recorded and monitored for possible abuse.

User Logon report

SOX requirements (Sec 302 (a)(4)(C) and (D) states that user accesses to the system be recorded and monitored for possible abuse.

Logon Failure report

The security logon failure includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

SOX requirements (Sec (a)(4)(C) and (D) – review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

Security Log Archiving Utility

Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.

Track Account management changes

Significant changes in the internal controls sec 302 (a)(6). Changes in the security configuration settings such as adding or removing a user account to an administrative group. These changes can be tracked by analyzing event logs.

Track Audit policy changes

Comply with internal controls sec 302 (a)(5) by tracking the event logs for any changes in the security audit policy.

Track individual user actions

Comply with internal controls sec 302 (a)(5) by auditing user activity.

Track application access

Comply with internal controls sec 302 (a)(5) by tracking applications process.

Track directory / file access

Comply with internal controls sec 302 (a)(5) for any access violation.

Appendix – GLBA

GLBA Compliance Reports

Section 501 of the GLBA documents specific regulations require for financial institutions to protect 'non-public personal information."

As part of the GLBA requirements, it is necessary that a security management process exist in order to protect against attempted or successful unauthorized access, use, disclosure, modification or interference of customer records. The organization must be able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive customer information.

User Logon report

GLBA Compliance requirements state that user accesses to the system be recorded and monitored for possible abuse.

User Logoff report

GLBA requirements state that user accesses to the system be recorded and monitored for possible abuse.

Logon Failure report

The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

GLBA requirements (review and audit access logs) call for procedures to regularly review records of information system activity such as audit logs.

Appendix – Security Reports

Security Reports

Successful and failed file access

Auditors are generally concerned with knowing who did what, and when. Monitoring file access can provide that information. This will be especially useful as companies attempt to comply with internal policies and industry regulations.

Successful logons preceded by failed logons

Multiple failed logins, followed by a successful login could indicate a successful breach by a hacker.

Audit log cleared events by user

A successful hacker will attempt to remove any trace of their attack. Their attempts to clear the audit logs are captured and can be displayed with this report.

Invalid logons by date

Allows you to identify days of heavy invalid logins. Many invalid logins over a weekend could indicate an attempt to penetrate the network.

Daily reboot statistics

Daily reboot statistics can help system administrators identify systems that might be having problems.

CPU load peaks by computers

CPU load peaks can indicate a system that is either configured incorrectly or one that is simply overworked. This can allow the system administrator to identify the system having problems and either fix the issues or transfer some of the workload (or justify new hardware).

Account usage outside of normal hours

This report can identify those accounts that are being used outside of normal (definable) hours of operations. Users occasionally work late, but frequent account usage after hours can indicate a security breach.

Audit policy history

Tracking audit policy on enterprise systems is a key function for security auditors. The 'Audit Policy History' report will show each systems audit policy for each date it was collected. This way compliance to the audit policy is documented and can be tracked.

Accounts that were never logged on

Part of an administrator's job is to deal with the clutter that collects in the NT4 SAM or Active Directory – or perhaps better stated, preventing it entirely. One of the more common sources of this clutter is redundant user accounts. In an effort to provide efficient service, those tasked with account creation often create new user accounts ahead of time for new employees or contractors. That way, when the new employee or contractor arrives, they can login and start to work immediately. In some organizations, this may mean dozens of accounts. Inevitably, job offers are declined or contractors' start dates postponed. The result is accounts that exist but have never been used. These accounts potentially represent a security risk because

- 1 They usually have a well-known default password set and
- 2 They may already have been placed in security groups pertaining to their job function.

An unscrupulous individual could login as the new account, set password to one of their own choosing and gain access to sensitive data by way of the accounts' group memberships. The 'Accounts that were never logged on' report can highlight these risky redundant accounts. Armed with this information follow-up e-mails can then be sent to the appropriate managers to determine what has transpired with the individuals for whom these accounts were created – i.e. did they really start work yet or not. Once the status of the employees is known, these accounts may then be disabled or deleted as required.

Administrative Access to Computers

Administrative access is required to perform many common tasks on workstations and servers. Such tasks include stopping and starting services, installing software and creating local groups for data permission. Care needs to be taken in the assignment of local administrative rights as clearly, an account with this right has a quite ranging ability to modify applications on SQL or IIS for example inappropriately assigned administrative access could lead to outages of business line applications.

On the other side of this equation are enterprising power users who will sometimes go out of their way to block administrators' legitimate access to their machines. These situations cause innumerable problems when it comes time to do remote managements, hardware and software inventory, software rollouts and even access control list updating. In either case, administrators need to get a sense of who has local administrative authority on workstations and servers in their environment. The 'Administrator Access by Computer' report can quickly provide this invaluable information.

File Access by User

Ensuring that appropriate permission is set on sensitive data is one side of the data security coin. The other is the process of auditing who is using the permissioned resources and when. There are times when it is important to know who the last person was to use their authorized access a resource. It is just as important to know if someone is trying to access a resource that he or she does not have access to.

Take the example of a spreadsheet containing salary information. 'Mary Hart' works in human resources and is authorized to access this information. Each time she accesses the file, if auditing is enabled, this access will be recorded to Windows' Event Logs as successful access. On the other hand, 'George hogan' is an employee in the mailroom, with some time on his hands. He spends this time browsing the network. Since he is part of the company' Administration Department, he has visibility of the department's shared files. He may be able to see a folder called 'Payroll Info' – when he tries to access this folder, however, he will receive the message 'Access Denied.' The fact that he unsuccessfully tried to access this folder will also be recorded to the Event Logs as a 'failed file access.'

The event log information described about is another distributed data source. Each files server maintains its own store of information on who accessed what file on that server and when. The challenge is to consolidate this information into one location and extract the most relevant transactions.

Hot fixes by Computer

Microsoft releases hot fixes on an almost weekly basis to remedy critical technical and security problems with the operating system. Clearly, these problems are considered serious enough that they might significantly disrupt a customer's business if not repaired. This puts pressure on administrators to keep close track of which hot fixes are installed on servers and workstations – an essential but potentially time-consuming task. Being able to poll computers on a scheduled (e.g. weekly) basis to verify which hot fixes they have installed means having on fewer balls to juggle.

Reporter's Hot Fixes by Computer report obviates the need to use a second tool to the collected hot fix information. The report interrogates the Registry of each workstation and server on the network to determine which hot fixes are installed. Like all of Reporter's reports, this process can be scheduled at whatever interval the administrator deems appropriate. This way, the hot fixes check becomes part of the administrator's standard list of scheduled audit reports. Frequent collection ensures that the most current information is always at hand.

Last logon by Domain Controller

As previously noted, identifying redundant user accounts is an important step towards achieving a secure network. We previously discussed the use of the 'user never logged on report' to highlight accounts that were created but have never been used. Another more frequent and common scenario is an employee or contractor leaves the organizations but IT is not notified. Though policies may be in place that stipulate that the accounts of departed staff are to be disabled and

eventually deleted – if IT doesn't know that someone had left they really have no way of knowing which accounts need to be disabled on a given day.

One indication of whether an account is being used or not is the 'last logon time.' Each time a user enters their username and password (either at logon time or as part of unlocking their workstation), a logon transaction is recorded and the time of that transaction is stamped on to that user's account. For the most part, if an account's last logon time is more than 2 to 3 weeks in the past (this takes into account possible employee vacations, training courses or travel), this is a good indication that the employee is not working with the company.

Reporter's 'Last Logon by Domain Controller' report is an authoritative source of users' last logon times. The report polls all domain controllers (DCs) for the last logon seen by that DC for each user and then calculates the most recent time for insertion into the report. As part of a regular security audit process, this report could be scheduled to run on at least a weekly basis. Armed with this report, follow-up e-mails can then be sent to the appropriate managers to determine what has transpired with the employees whose accounts appear in the report – i.e. have these staff left the company or are they on some extended leave. Once the status of the employee is known, these accounts may then be disabled or deleted as required.

User Account Locked Out

User account lockouts occur when a user incorrectly enters password several times in succession. In most organizations, a user who enters their password incorrectly three times will have their account locked out (i.e. be barred from accessing the network) for some defined time period (e.g. 15 minutes) or possibly, indefinitely.

Frequent user account lockouts can result from clumsy or forgetful users but they may also be an indication of someone trying to gain unauthorized access to the network using their own or someone else's account. Like file and resource access, account lockouts are recorded in Windows' Event logs of each server that authenticates user access. Once again, the challenge is to pull this information together.

Reporter's User Account Locked Out report extracts lock out events from all the data collected from servers across the company effectively mining out the transactions that might indicate suspicious activity. As part of the regular audit process, it would be advisable to schedule the execution of this report in the early morning hours just prior to start of business (e.g. at 6 a.m.).

This would highlight to the administrator or security officer all accounts that were locked during the overnight period. Careful review of the report could help to determine if sleepy users caused the lockouts or someone trying to hack into the network at night. Another business use of this information can be to provide some insight into Help Desk call volumes. If, on a given day, there was a large increase in calls to the Help Desk, a quick perusal of the account lockout report might provide at least part of the explanation for the increase.

Appendix – BASEL II

BASEL II

In the financial services industry, nothing is more than the trust of customers, shareholders, partners and regulators. The risk management officer's primary task is to ensure trust is sustained through a systematic risk management program.

BASEL II defines operational risk, one of the pillars of the Accord, as 'the risk of direct or indirect loss resulting from the inadequate or failed internal process or systems or from external events.'

If your company eventually intends to adopt the Advanced Measurement Approach (AMA), then you are required to measure aspects of operational risk, such as IT security.

It involves two steps. First, ensure that appropriate permission is set on sensitive data. Secondly, during the auditing process the user needs to have permission on the resources accessed at a particular point in time. There are times when it is important to know who was the last authorized person who had access to the resource. It is just as important to know if someone is trying to access a resource that he or she does....

Appendix – FISMA

FISMA

FISMA requires detailed annual E-Government security reports of all federal agencies. As to fulfill FISMA requirements, the agencies should implement the FISMA requirements and transmit the corresponding reports to Office of Management and Budget (OMB) by October of each year. According to the sections **FISMA Sec. 3505** and **FISMA Sec. 3544**, the transmitted reports should summarize the following requirements to comply with FISMA.

FISMA Sec. 3505

Sec.3505.(c)(1) - Maintenance and results of major federal information systems or applications inventory security of the agency.

Sec.3505.(c)(2) - Inventory of networks interfaces not only within the agency, but also the network of other agencies or contractors working under the agency.

FISMA Sec. 3544

Sec.3544.(a)(1)(A)(i) - Information security protection against unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems of the agency.

Sec.3544.(a)(1)(A)(ii) - Information security against unauthorized usage risks of the contractor or other organizations working on behalf of the agency.

Sec.3544.(a)(1)(A)(ii) - The responsibility of the head while the major federal systems operated either by the agency or by the contractor and other agencies under the agency.

Sec.3544. (b) - Integrity, authenticity, availability of the systems supporting the agency operations and assets.

Sec.3544. (b)(2)(C) - Detailed reporting on the existing risks and remedial actions. Effectiveness of Information Assurance program and progress in remedial plans and actions.

Sec.3544. (b)(2)(D) – Periodical risk management reporting. Accurate report on the current FISMA compliance status. Annual information on security training and Internet security training for the agency personnel and also the contractor.

Appendix – PCI DSS

PCI DSS

PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or they risk losing the ability to process credit card payments.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

Glossary

Term	Description
Agent Configuration	Process of configuring the system for reporting to multiple managers, to filter events, to monitor services, software installations, processes, system health, and to archive the events database.
Alert Configuration	Process of configuring alert notifications in the form of Sound, E-mail, Console message or any Custom action.
Alerts	A feature that instructs programs that notify timely information about the events.
Analyzing Event Traffic	The process to analyze the event traffic patterns. The data can be used to filter out irrelevant events and perform other operation tasks.
Audible Alert	A feature that instructs programs that usually notifies information by sound.
Auto Discover Mode	Process of adding computers from your network automatically.
Change Audit	An application that used to track the occurred changes on a computer's file system and registry and provides you with a lifeline to restore it back to a working configuration.
Change Management	The process that enables the user to monitor, analyze, understand, and recover from change.
Console Message Alert	A feature that instructs programs that usually notifies information to the selected machine.
CPU Performance	A term used to monitor the CPU performance.
CRL	A CRL is a list identifying revoked certificates, which is signed by a CA and made freely available at a public distribution point.
Custom Alert	A feature that instructs programs to execute custom action on receipt of an event.
Disk Space Usage	A term used to monitor the disk space usage.
E-mail Alert	A feature that instructs programs that usually notifies information by E-mail.
Event Filtering	Process of filtering the events that are not important. Monitoring unimportant events cause the database to occupy more disk space.

Term	Description
Event Information	A window pane that displays the summary of event details in the EventTracker Management console.
Event Logs	A type of event message. The event logs are recorded whenever certain events occur, such as services starting and stopping, or users logging on and off and accessing resources.
Event Monitoring	A window pane that displays the real-time event information in the EventTracker Management console.
EventBox	An archived event data file. You can create an EventBox by using EventVault Warehouse Manager console.
EventTracker	An application that can be used to centrally monitor, analyze, and manage events being emitted by Windows 2000/2003/2008/2008 R2 /XP /Win 7/ Vista UNIX systems, and SNMP enabled devices.
EventVault	The console used to archive the events from EventTracker database. EventVault can operate in Automatic Archival and EventBox on demand methods.
Exclude List	The process to configure the network connections that need not to be monitored.
Filters	The process to filter out events that you do not want to monitor.
Include List	The process to configure the network connections to monitor. Include list Network connections always override the Exclude list Network connections.
IP Subnet	A 32-bit address used to identify a node on an IP internet. The address is typically represented with a decimal value of each octet separated by a period. For example: 192.168.7.27.
Knowledge Base	A Web site containing information about Windows events and custom EventTracker events.
Flex Report	Process of analyzing the event details by setting criteria such as date range, time range, rule, and computer.
Log Backup	A backup that copies event logs automatically in the EventTracker Agent directory whenever the event logs are full.
Logfiles	The process to monitor textual log files such as SQL or ISA logs, created by any vendor. You can also configure the strings to search. If any record matching the search string is found, an event will be generated.

Term	Description
Manager Configuration	It comprises of various options to configure Alert events, Keyword indexing, Syslog/virtual collection point, Direct Log Archiver / NetFlow Receiver, Agent File transfer settings, configuration assessment settings, SMTP server settings and StatusTracker settings.
Memory Usage	A term used to monitor the memory usage.
Monitor Syslog	The process to monitor Syslog being sent by an UNIX system.
NetFlow	A Cisco-proprietary IP statistics collection feature that collects information on IP flows passing through a router.
Quick Statistics	The process to view the summary of event statistics such as Total events received, Total alerts received, Total systems monitored, and so on.
SNMP Event Manager	An application called TrapTracker used to monitor and manage critical traps emitted by network devices in your enterprise.
SNMP Traps	The process to receive trap messages generated by local or remote SNMP agents and forwards the messages to third party vendor software such as an NOC.
StatusTracker	An application used to monitor the status of your IT resources and provides you various reports.
Syslog Receiver	The process to set the SYSLOG receiver. After setting this option, the Manager will receive any SYSLOG being sent by an UNIX system.
System Information	The process to collect and view the system configuration information. You can view the information of System Summary, Hardware Resources, Components, Software Environment, Internet Settings, and Applications.
System Manager	A console helps you to manage groups, systems, and Agents.
System Performance	The process to monitor the system performance in graph, histogram, or report form.
System Statistics	A window that displays the system statistics in EventTracker Management console.
TCP	Transmission Control Protocol. TCP is responsible for verifying the correct delivery of data from Agent to server. TCP adds support to detect errors or lost data and to trigger transmission until the data is correctly and complete received.

Term	Description
UDP	User Datagram Protocol. A connectionless protocol that, like TCP, runs on top IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network.
Vulnerability	Vulnerabilities are weaknesses in process, administration, or technology that can be exploited to compromise your IT security.
Vulnerability Parsers	The parser reads the XML report generated by Vulnerability scanners and extracts vulnerability information from it.
Vulnerability Scanners	A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses.

Index

A

About	xv
Active Alerts	480
activities per system	100
Add-in Software Modules	
Solaris Agent	665
StatusTracker	664
TrapTracker	664
WhatChanged	664
Agent	
advanced filters	373
applying settings	420
backup configuration	422
basic configuration	357
event delivery mode	362
filtering events	369
filtering events with exception	370
Installing	342
multiple destinations	358
pre-installation procedures	342
protecting configuration	423
Removing client components	353
SID translation	376
system health	377
Uninstalling	350
Upgrading	352
version	334
Agent Management Tool	501
accessing	501
Agent Service	
restart	331
status	333
Agent service status	
all 504	
group	503
system	502
Agent service version	
all 508	
group	507
system	507
Agentless Monitoring	436
adding	436
Alert Actions	
edit	231
Alerts	212
delete	222
manager side actions	222

application activity	111
Assessment Results	613
Asset Value	335

B

Benchmarks	
importing	633

C

Category Groups	449
creating	449
deleting	450
managing	450
modifying	450
CCE	606, 607
Choosing Columns	184
Collection Master	
Collection Point details	553
configuring port	554
deleting CABs	554
deleting Collection Point details	555
starting	552
Collection Point	
adding Collection Masters	558
deleting Collection Master settings	559
editing Collection Master settings	559
starting	557
viewing CAB status	559
Collection Point model	547
scalability	547
scenarios	547
Column Name	250
Compliance	
BASEL	674
FISMA	675
GLBA	669
HIPAA	666
PCI DSS	676
Security Reports	670
SOX	667
Configure	
Agent File Transfer	205
Alert notification tracking	188
Audible Alerts	223
Categories as Alerts	221
Config Assessment	205

Console message Alerts	224
correlation receiver.....	190
Custom action.....	229
custom Alerts	213
DLA	198
E-mail Alerts.....	222
E-mail settings.....	205, 209
event filters.....	237
event filters with exception.....	239
Forwarding events as SNMP Traps.....	226, 227
NetFlow Receiver	203
purge Alert events cache	188
remedial actions.....	189
RSS Alerts	225
SYSLOG receiver.....	193
CPE.....	606, 608
CPE results.....	617
Custom Column	263, 270, 278, 281, 289, 291, 295
Custom Logon Message	192
CVE.....	606, 607
CVSS.....	610

D

Deviation	621
Diagnostic and Support	
debug levels	465
diagnostic alert.....	471
obfuscating	467
Discover Modes	320
Auto	320
Manual	321
Display Name.....	251
DSCP	169
Duplicate Alerts	189
suppress.....	189

E

Encryption	417, 558, 661
agent	662
CP	662
Enterprise Activities	
dashlets.....	90
monitoring	90
Event Categories	
Alerts	454
creating	451
deleting	453
modifying	452
Event Details	

deleting.....	453
Event Traffic Analysis	
category.....	492
correlate.....	493
custom.....	495
event id	494
Event-O-Meter	30
events by occurrences	107
EventTracker	
about.....	19
services and ports.....	20
starting	22
EventTracker Components	
Diagnostic & Support.....	462
EventVault Manager.....	32
Knowledge Base.....	34
System Manager.....	319
EventTracker NetFlow Analyzer....	170
benefits.....	170
EventTracker NetFlow Receiver	171
EventTracker Parsers	
eEye Retina.....	201
Nessus	200
Qualys	199
Rapid7 NeXpose.....	202
SAINT.....	200
EventTracker Services	
Event Correlator.....	20
EventTracker Agent	20
EventTracker Alerter	20
EventTracker EventVault.....	20
EventTracker Indexer.....	20
EventTracker Receiver	20
EventTracker Remoting.....	21
EventTracker Reporter.....	21
EventTracker Scheduler.....	21
WcwService	21
EventTracker users list	37
EventVault	
appending CABs	485
backup.....	458
configuring.....	444
deleting EventBox.....	460
extracting EventBox.....	459
moving CABs	460
saving EventBox information	458
verifying EventBox integrity.....	445
viewing CABs.....	444
Exit.....	38
Export	
Alerts.....	474
Categories.....	472
Domains.....	475
Filters.....	473

RSS Feeds 476, 477
Scheduled reports 476
Exporting 298, 619, 633

F

Favorites 29, 167
FDCC 604
 report bundle 626
 reporting format 611
Filtering Events
 advanced filters 373
FISMA
 sec 3505 675
 sec 3544 675

G

GLBA
 audit logs access 669
 logon failure 669
 user logoff 669
 user logon 669

H

HIPAA
 audit logs access 666
 logon failure 666
 user logoff 666
 user logon 666

I

ifIndex 169
Import
 Alerts 479
 Categories 478
 Domains 480
 Filters 479
 RSS Feeds 483, 484
 Scheduled reports 482
IP addresses by traffic 100

K

Keyword Indexer
 benchmark 658
 overview 658
Keyword Indexing 190
keywords 655

Knowledge Base 192

L

Legacy Reports 29, 516
Limit to time range .. 260, 288, 289, 291,
 292, 293
log on failure activity 108
Log Search 657
 advanced 659
 basic 659
Log Volume 303, 305, 306
Logical System Groups 325
 IP Subnet 326
 Manual selection 327
 System Type 325
Logo 31

M

Manual Mode
 Adding a group of computers 323
 Adding a group of computers - IP
 subnet 324
 Adding a single computer 321
Monitoring
 applications 380
 Check Point logs 396
 excluding network connections 402
 filtered processes 415
 filtering applications not to monitor
 381
 filtering applications to monitor 382
 filtering services not to monitor 384
 including network connections 406
 log backup 415
 logfiles 384
 network connections 400
 processes 414
 searching strings 392
 services 382
 suspicious connections 409
 Trusted List 409
 VMware logs 398

N

Netflow
 application 173
NetFlow
 interface manager 175
 protocol 173
 traffic destination 174

traffic source.....	174
utilization	175
volume.....	175
network activity	111
NIST.....	600
benchmarks.....	601
non-admin user.....	93

O

OVAL	607, 609
OVAL definitions.....	615

P

Patch results.....	618
Person Hour.....	311
Personalization	
resetting.....	140
processes by occurrence.....	104

Q

Queued	162, 277, 280, 284, 298, 300, 305, 308
Quick View.....	263, 269, 300

R

Reg-ex	246
Remedial Action.....	230
Replacing outdated CRL.....	34
Report Calendar	29, 164
Report Status.....	29, 166
Restarting Agent service	
all 506, 508	
group	505
system.....	505
Results Summary Console	
configuration policy dashboard.....	583
Risk Metrics	212
ROI	311
RSS Feeds	315
adding.....	315
deleting	317
runaway process activity	109

S

SCAP	605
------------	-----

content.....	606
Scheduler service	443
Security Dashboard	
configuring category dashlets	134
customizing.....	138
viewing.....	131
Security Reports	
account usage outside of normal	
hours.....	670
accounts that were never logged on	
.....	671
administrative access to computers	
.....	671
audit log cleared events by user	670
audit policy history	671
CPU load peaks by computers	670
daily reboot statistics	670
file access by user.....	672
hot fixes by computer.....	672
invalid logons by date.....	670
last logon by Domain Controller	672
successful and failed file access.....	670
successful and logons preceded by	
failed logons.....	670
user account locked out	673
Separator	251
Server Hardening.....	661
Severity Mapping	
eEye retina.....	202
nessus	200
Qualys	199
Rapid7 NeXpose.....	203
saint.....	201
software activity.....	110
SOX	
account management changes	668
application access.....	668
audit logs access.....	667
audit policy changes	668
directory / file access	668
individual user actions	668
logon failure.....	667
security log archiving utility	667
user logoff	667
user logon.....	667
Standard Column....	255, 265, 274, 277, 280, 284, 288, 290, 294, 296
Summary.....	43
Suspicious Connections	408
Suspicious Traffic	307, 308, 310
System Details.....	330
System Report.....	432
all 434	
managed system	433

unmanaged system434

T

Tag Clouds652
Terminator251
Trusted List
 adding programs412
 firewall exceptions413
Tuning Alerts..... 44

U

Understaing filers and filter
 exceptions239
USB378
USB activity113

V

Virtual Collection Points194
 architecture.....194
 configuring EventTracker Receiver .195

forwarding raw syslog messages... 196
syslogs195
Windows events196
Vista Agent354
 prerequisites355
VistaAgent
 event consumers355
 event logs and channels.....354
 event publisher354
 EVTX.....356
 filtering events.....356
Vulnerability
 scanners199

W

Weights
 multiple tags655
 tag653

X

XCCDF607, 609